SIEMENS

SIMATIC NET

Industrial Ethernet Wireless LAN
RLM Manager
CP 1515 Manager

Manual

C79000-G8976-C171-01
Release 11/2001

Copyright Siemens AG 2001

All rights reserved

The reproduction, transmission or use of this document or its contents is not permitted without express written authority. Offenders will be liable for damages. All rights, including rights created by patent grant or registration of a utility or design, are reserved.

Disclaimer

We have checked the contents of this manual for agreement with the hardware and software described. Since deviations cannot be precluded entirely, we cannot guarantee full agreement. However, the data in this manual are reviewed regularly and any necessary corrections included in subsequent editions. Suggestions for improvement are welcome.

Siemens AG 2001
Bereich Automatisierungs- und Antriebstechnik
Geschäftsgebiet Industrie-Automatisierungssysteme
Postfach 48 48, D-90327 Nürnberg

C79000-G8976-C171-01
© Siemens AG 2001
Subject to technical change.

Siemens Aktiengesellschaft

Classification of Safety-Related Notices

This document contains notices which you should observe to ensure your own personal safety, as well as to protect the product and connected equipment. These notices are highlighted in the manual by a warning triangle and are marked as follows according to the level of danger:

NOTE:

Highlights important information on the product, using the product, or part of the documentation that is of particular importance and that will be of benefit to the user.

WARNING:
Indicates that death or severe personal injury can result if proper precautions are not taken.

CAUTION:
with warning triangle Indicates that minor personal injury can result if proper precautions are not taken.

CAUTION:

without warning triangle indicates that damage to property can result if proper precautions are not taken.

Trademarks

SIMATIC®, SIMATIC NET® and SINEC® are registered trademarks of Siemens AG.

Third parties using for their own purposes any other names in this document which refer to trademarks might infringe upon the rights of the trademark owners.

Safety Instructions Regarding your Product

Before you use the product described here, read the safety instructions below thoroughly.

Qualified Personal

Only qualified personnel should be allowed to install and work on this equipment . Qualified persons are defined as persons who are authorized to commission, to ground, and to tag circuits, equipment, and systems in accordance with established safety practices and standards.

Correct use of Software Products

Please note the following:

Caution

This software may only be used for the applications described in the catalog or the technical description, and only in connection with software products, devices, or components from other manufacturers which have been approved or recommended by Siemens.

Before you use the supplied sample programs or programs you have written yourself, make certain that no injury to persons nor damage to equipment can result in your plant or process.

Prior to Startup

Before putting the product into operation, note the following warning:

Caution

Before installation and startup, read the instructions in the appropriate documentation. For ordering data of the documentation, please refer to catalogs or contact your local Siemens representative.

Preface

Purpose of the Operating Instructions

These Operating Instructions support you when configuring, commissioning, and troubleshooting networks including the Industrial Ethernet Wireless LAN RLM Manager and CP 1515 Manager.

Further Documentation

The manuals

- "SIMATIC NET Industrial Ethernet Twisted Pair and Fiber Optic Networks"
- "SIMATIC NET Industrial Ethernet Wireless LAN, Basics"
- "SIMATIC NET Industrial Ethernet Wireless LAN, RLM"
- "SIMATIC NET Industrial Ethernet Wireless LAN, CP 1515"

are containing information on other SIMATIC NET products that you can operate in conjunction with RLM Manager and CP 1515 Manager in an Industrial Ethernet network.

All manuals are provided on the CD-ROM "SIMATIC Net Wireless LAN, Systemsoftware and Manuals" that was included with your product.

Guide to the Manual

To help you to find specific information quickly, these manual includes the following parts:

- At the front of the operating instructions you will find a complete table of contents.
- At the back of the operating instructions, you will find an index with which you can find topics quickly.
- In the Manual "Industrial Ethernet Wireless LAN, Basics" you will find a Glossary in which the most important specialist terms used in the instructions are defined.

Audience

These Operating Instructions are intended for persons involved in configuring, commissioning, and troubleshooting networks including the RLM, CP 1515, RLM Manager -, and CP 1515 Manager.

Personal Qualification Requirements

Only qualified personnel should be allowed to install and work on this equipment.
Qualified personnel as referred to in the operating instructions or in the warning notes are defined as persons who are familiar with the installation, assembly, startup and operation of this product and who possess the relevant qualifications for their work, e.g.:

- Training in or authorization for connecting up, grounding or labeling circuits and devices or systems in accordance with current standards in safety technology;
- Training in or authorization for the maintenance and use of suitable safety equipment in accordance with current standards in safety technology;

Contents

1 Introduction

1.1 About Siemens SIMATIC NET Industrial Wireless LAN 16

1.2 About Siemens SIMATIC NET Industrial Wireless LAN Tools..... 17
1.2.1 CP 1515 Manager 19
1.2.2 RLM Manager 19

1.3 About SIMATIC NET Industrial Wireless LAN RLM 20

1.4 About This Manual 21
1.4.1 About Icons used in this Document..... 22
1.4.2 On-line Help Documentation..... 22
1.4.3 Additional Files on your CD-ROM 23
1.4.4 Other Sources of Information 23

2 Wireless Configurations

2.1 Introduction 24

2.2 Peer-to-Peer Workgroup..... 25

2.3 Basic Infrastructure 26
2.3.1 Stand Alone Configuration 26
2.3.2 Wireless Access to Ethernet Networks..... 27

2.4 Advanced Infrastructures 29
2.4.1 Multiple Channel Configuration..... 29

3 Setting Up your LAN Administrator Station

3.1 Introduction 32

3.2 Assigning an LAN Administrator Station 34
3.2.1 Minimum Requirements 34

3.3 Managing Peer-to-Peer Workgroups 35

3.4 Managing Infrastructure Networks..... 36
3.4.1 Wired or Wireless?..... 36

3.5 Installing SIMATIC NET IWL Software 40
3.5.1 CP 1515 Manager 40
3.5.2 RLM Manager 41
3.5.3 Installing RLM Manager 42

3.6 Configuration Scenarios 47
3.6.1 Wired LAN Administrator Station..... 47
3.6.2 Wireless LAN Administrator Station 50

3.7 Uninstalling SIMATIC NET IWL Software..... 54

4 Basic Network Configuration

4.1 Introduction 55
4.1.1 Peer-to-Peer Workgroups..... 55
4.1.2 Infrastructure Networks 56

4.2 Configuring Infrastructure Networks 58
4.2.1 Basic Configuration 58

5 Monitoring your SIMATIC NET IWL Network

5.1 Introduction 67
5.1.1 SIMATIC NET IWL Tools 67
5.1.2 Which Tool Should You Use? 68

5.2 Using the CP 1515 Manager 71
5.2.1 Monitoring Methods 71
5.2.2 Link Test Window 74
5.2.3 Site Monitor Window 81
5.2.4 Logging Measurement Data 92
5.2.5 Diagnose Card 96
5.2.6 Troubleshooting Site Monitor 96

5.3 Using the RLM Manager 98
5.3.1 Monitoring Options 98
5.3.2 Connecting to Access Points RLMs 99
5.3.3 System Information 101
5.3.4 Remote Link Test Window 103
5.3.5 Remote Statistics Tab 108
5.3.6 System Intervals 112

6 Optimizing Performance

6.1 Introduction 116

6.2 Eliminating Redundant Traffic 117
6.2.1 Protocol Filtering 118
6.2.2 Do You Need Protocol Filtering? 118
6.2.3 Filtering Network Protocols 120
6.2.4 Optimizing Wired Connections 121
6.2.5 Checking the Cable System 122
6.2.6 Checking the Length of Your LAN Segments 124
6.2.7 Optimizing Wireless Connections 125
6.2.8 Diagnosing Link Quality 126
6.2.9 Link Integrity 144

6.3 Designing High Capacity Networks 146
6.3.1 About the CSMA/CA Protocol 146

7 Security

7.1 Introduction 154

7.2 Securing Access to Wireless Data 155
7.2.1 Restrict Wireless Access to the Network 155
7.2.2 Closing the Wireless Network 156
7.2.3 Access Control 159
7.2.4 Enabling Access Control 160
7.2.5 Creating/Editing an Access Control Table 161
7.2.6 Importing an Access Control Table 163
7.2.7 Disabling Access Control 164
7.2.8 Enabling RADIUS Server Access Control 165

7.3 Wireless Data Encryption 167
7.3.1 Enabling WEP Encryption 168

7.4 Securing Access Point RLM Setup 177
7.4.1 Read and Read/Write passwords 177
7.4.2 SNMP IP Access List 178
7.4.3 Trap Host Alerts 180

7.5 Advanced Security Maintenance 183
7.5.1 Maintaining Access Control Tables 183
7.5.2 Maintaining WEP Encryption Keys 183

8 Advanced Network Configurations

8.1 Introduction 190

8.2 Advanced Parameters 191
8.2.1 Advanced Parameters 192
8.2.2 Bridge Parameters 197
8.2.3 Access point IP Parameters 207
8.2.4 SNMP Parameters 211
8.2.5 Ethernet Interface 216

8.3 Configuring Large Networks 218
8.3.1 Common Parameters 219
8.3.2 Unique Parameters 220
8.3.3 Managing Configuration Consistency 220

8.4 Modifying the Configuration 226
8.4.1 Changing Common Parameters 227

8.5 Restoring a Back-up Configuration 228

8.6 Dual PC Card Configuration 229

8.7 About IP Addresses and Subnets 229
8.7.1 BOOTP and DHCP 231

A Start-up Configuration

A.1 Introduction 232

A.2 Factory-set Configuration 233

B Troubleshooting

B.1 Introduction 236
B.1.1 Problem-solving Approach 236

B.2 Rebooting RLMs 241
B.2.1 Manual Reboot 241
B.2.2 Remote Reboot 243

C Forced Reload Procedure

C.1 Introduction 244

C.2 Doing a Forced Reload 246
C.2.1 Step 1 - Preparations 246
C.2.2 Step 2 - Set to “Forced Reload” Mode 249
C.2.3 Step 3 - Configuring and Uploading Files 250
C.2.4 Creating a Back-up File 257

D Upgrading the RLM Software

D.1 About the RLM Software 258

D.2 Upload Software 259
D.2.1 Confirm Upload RLM Software 260
D.2.2 Upload Software, a Look under the Hood 261

E Further Support

E.1 Who to contact 262

E.2 Automation and Drives, Service & Support 263

E.3 Service & Support on the Internet 266

E.4 Training for SIMANTIC NET 267

E.5 Certification 267

Glossary 268

Index 293

1 Introduction

1.1 About Siemens SIMATIC NET Industrial Wireless LAN

The Siemens SIMATIC NET Industrial Wireless LAN (IWL) product family is a comprehensive set of network equipment that enables you to build any type of network configuration, from a small independent wireless network to a large, completely wireless infrastructure. The Siemens SIMATIC NET Industrial Wireless LAN product family consists of an RLM to connect wireless stations to existing Ethernet LAN infrastructures.

The wireless network interface is not much different from the interface for wired LANs. The operating system will not even notice the difference.

The wireless network interface supports all protocols that are supported by standard Ethernet adapter cards. Like wired network interfaces, wireless network interfaces are installed with a dedicated SIMATIC NET Industrial Wireless LAN driver, but unlike wired network interfaces, wireless network interfaces do not need a cable to connect them to the network. Only wireless network interfaces allow you to relocate workstations without the need to change network cabling or connections to patch panels or hubs.

1.2 About Siemens SIMATIC NET Industrial Wireless LAN Tools

The Siemens SIMATIC NET Industrial Wireless LAN software suite consists of a set of management tools that enables you to:

- Display and modify the configuration of (remote) network components.
- Configure network components such as Radio Link Modules.
- Diagnose the network performance and, if necessary, identify and solve network errors.
- Manage and optimize network performance.

The Siemens SIMATIC NET Industrial Wireless LAN software suite consists of the following tools:

- CP 1515 Manager
- RLM Manager

The Siemens SIMATIC NET Industrial Wireless LAN tools can be installed on stations that run the Microsoft Windows 98 , ME, NT v4.0 or 2000 operating systems.

NOTE:

The Siemens SIMATIC NET Industrial Wireless LAN products have been designed for interoperability with all other wireless LAN products that use the direct sequence radio technology, as identified in the IEEE 802.11 standard for wireless LANs.

Your SIMATIC NET Industrial Wireless LAN hardware will communicate with other vendors' IEEE 802.11 compliant wireless LAN products.

However, you may not always be able to use the SIMATIC NET Industrial Wireless LAN software suite in combination with other vendors' products, due to the following reasons:

- The IEEE 802.11 standard for wireless LANs does not identify standards for diagnostic or management tools; i.e. each vendor may have designed a customized tool to configure and/or manage the IEEE 802.11 wireless network.
- The Siemens SIMATIC NET Industrial Wireless LAN software suite has been designed to offer an enhanced set of tools to monitor and analyze a wide range of diagnostic tallies.

  Some of these tools require additional functions in the hardware that (by default) is supported by all Siemens SIMATIC NET Industrial Wireless LAN products, but may not be supported by the other vendors' products.

If other vendors' products do not allow you to display communications quality or configuration parameters using the SIMATIC NET Industrial Wireless LAN software suite, please refer to the documentation that was shipped with the other vendors' product.

1.2.1 CP 1515 Manager

The CP 1515 Manager is a diagnostic tool to monitor wireless radio communication between a wireless station and its Access Point RLM, or to monitor the link between two wireless stations in an independent network.

Furthermore it can be used as a site monitor to show the coverage of the installed Access Point RLM in a certain area.

1.2.2 RLM Manager

The RLM Manager is primarily a tool for LAN administrators or system supervisors. You can use the RLM Manager program to configure Radio Link Modules (RLMs) and to monitor the performance of your wireless network. It can be run on any station in the network, either wired or wireless.

1.3 About SIMATIC NET Industrial Wireless LAN RLM

The Radio Link Module RLM is a transparent bridge device equipped with two PC Card slots A and B. Wireless Network Interfaces A and B are corresponding to slot A and B of the RLM, into which PC Cards CP 1515 can be inserted.

The Access Point RLM is identified by either one of the following MAC addresses:

- The universal MAC address of (one of) the Wireless Network Interface(s) used by the Access Point RLM, or
- The universal MAC address of the Ethernet Interface.

For information concerning all Siemens SIMATIC NET Industrial Wireless LAN products, please refer to the documentation that was included with your product, or visit our **http://www.siemens.com/mobic**.

1.4 About This Manual

This Manual describes how to use the SIMATIC NET Industrial Wireless LAN (IWL) tools to configure and monitor wireless LANs built with SIMATIC NET IWL products.

In this manual, you will find the following:

- 1 “Introduction” describes the SIMATIC NET Industrial Wireless LAN tools and the sources for finding more information.
- 2 “Wireless Configurations” describes network scenarios that will be used throughout this document.
- 3 “Setting Up your LAN Administrator Station” describes how to select a station to manage your SIMATIC NET Industrial Wireless LAN network, and how to install the necessary software.
- 4 “Basic Network Configuration” explains how to configure your particular network, using three network scenarios, from simple to sophisticated.
- 5 “Monitoring your SIMATIC NET IWL Network”, describes how to monitor and diagnose communications quality.
- 6 “Optimizing Performance” presents a number of considerations to help you sort through the complex factors that determine the performance of your wireless LAN.
- 7 “Security” describes how to enhance security and minimize unauthorized use of your SIMATIC NET Industrial Wireless LAN network.

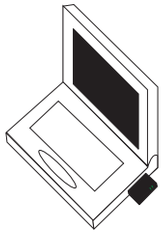
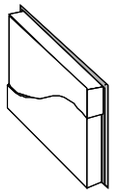
This document does not describe every possible option supported by the SIMATIC NET Industrial Wireless LAN software suite. It should serve as a

general guideline to help you to decide which tool can help you to accomplish a specific task.

For more information about specific software screens or options, you are advised to consult the on-line help documentation.

1.4.1 About Icons used in this Document

Throughout this document we use the following icons to represent the various networking devices:

Icon	Description
	Wireless computer Equipped with: • PC Card (CP 1515)
	Access Point (Radio Link Module RLM) Equipped with: • one or two PC Card (CP 1515)

1.4.2 On-line Help Documentation

Information about specific software screens or options in your RLM Manager or CP 1515 Manager program is covered in the on-line help of the programs.

- To access context-sensitive help on a specific screen for the SIMATIC NET Industrial Wireless LAN programs, click the **Help** button or press the F1 function key.
- In the on-line help you can click the **Contents** tab to get an overview of the on-line information, or click the **Index** tab to open an alphabetical list of specific topics.

Product specifications are listed in the Manual that came with your SIMATIC NET Industrial Wireless LAN products.

1.4.3 Additional Files on your CD-ROM

The CD-ROM that is shipped with your SIMATIC NET Industrial Wireless LAN products include a file called "readme.rtf." This file contains information about the version of the software and/or drivers on the CD-ROM.

You are advised to read this file prior to installing your SIMATIC NET Industrial Wireless LAN products, as it may contain additional information that was not available when this document was produced. You can also download or view the "readme.rtf" file on the Siemens **http://www.siemens.com/mobic** web site.

1.4.4 Other Sources of Information

For information on updates and other Siemens news, see the **http://www.siemens.com/mobic**.

For technical support, please consult Further Support (page 262).

2 Wireless Configurations

2.1 Introduction

This document describes a number of network scenarios that may serve as an example for building your wireless system.
Wireless systems typically apply to indoor network environments that require connectivity for devices roaming throughout the network environment.

Wireless systems are wireless networks that service wireless (mobile) devices. Wireless devices may roam freely throughout the network, with the only restrictions being the size and distance of the wireless LAN.

Subject to the size and requirements of your LAN, a wireless system can be identified by either one of the following type of configurations:

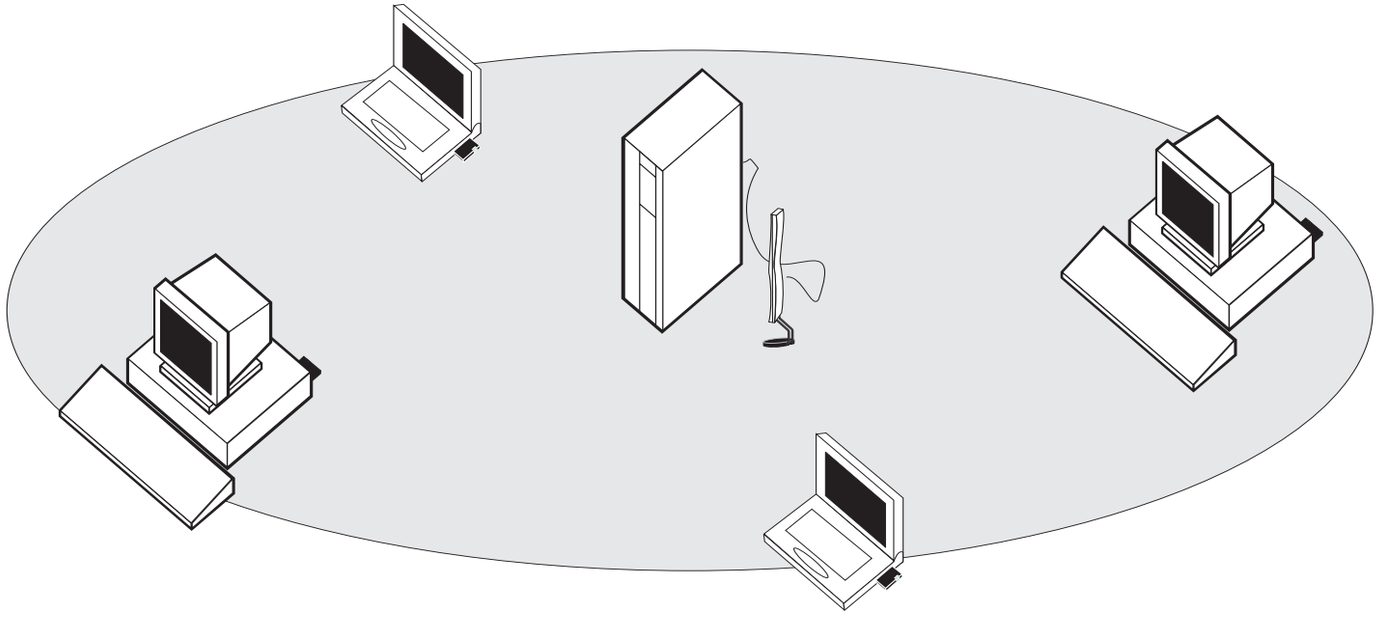
- Peer-to-Peer Workgroup
- Basic infrastructure
    1. Stand alone configuration
    2. Wireless access to Ethernet networks
- Advanced infrastructures
    1. Multiple channel configuration

2.2 Peer-to-Peer Workgroup

A Peer-to-Peer workgroup, as pictured in Figure 1, is a group of wireless devices that do not bridge their data via the Radio Link Module (RLM). All machines within a Peer-to-Peer network are configured to “Peer- to-Peer” mode.

The most simple independent network is one without a server, where stations communicate Peer-to-Peer, e.g. by sharing a disk or printer via Microsoft Networking.

Figure 1 Peer-to-Peer Workgroup



Peer-to-Peer networks are typically used for small networks where:

- All wireless stations participate in workgroup computing, for example using the disk-sharing option of Microsoft Networking and Printers.
- All stations are within range of a wireless server.

Peer-to-Peer networks are a quick and easy solution to set up a wireless network at trade-shows, business visits or other (off-site) locations.

2.3 Basic Infrastructure

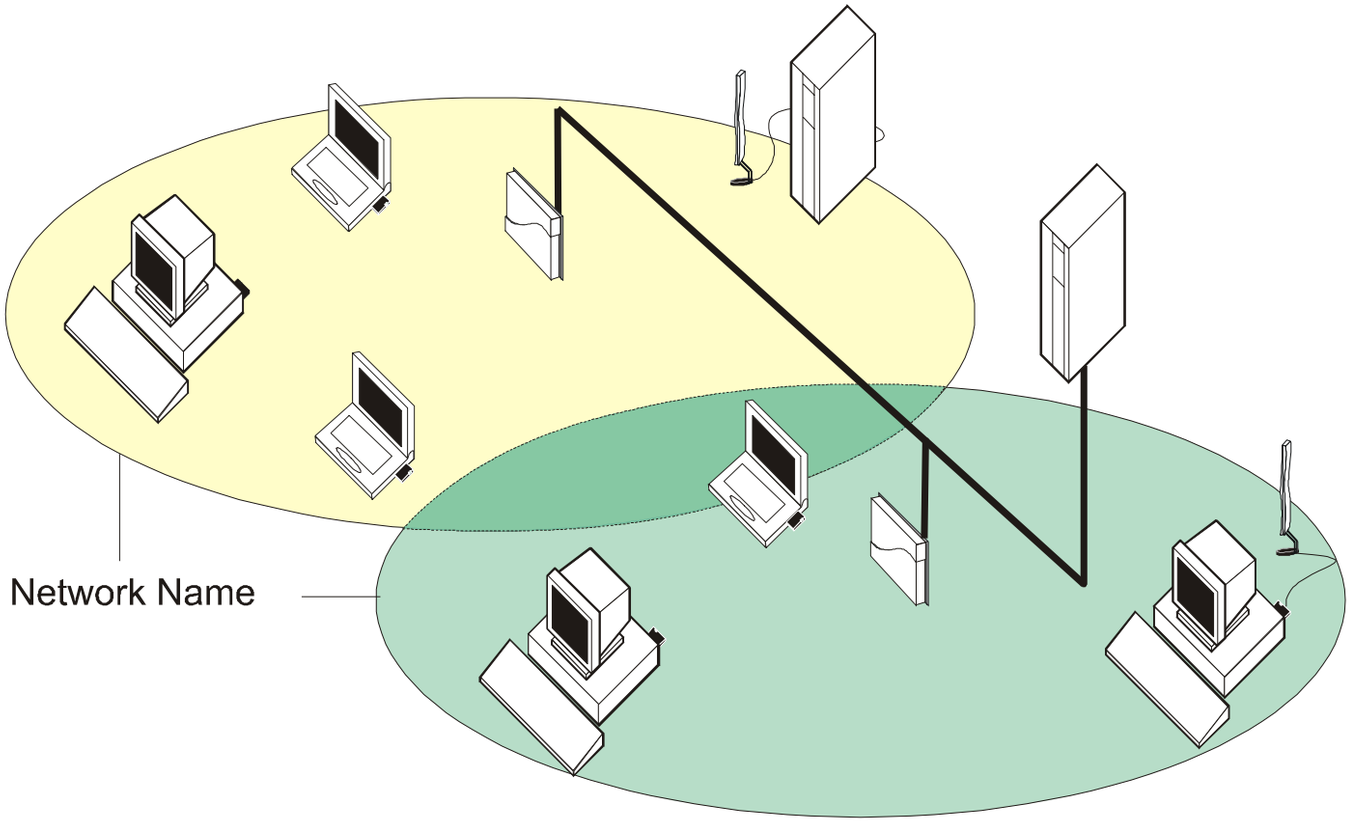
2.3.1 Stand Alone Configuration

In a stand alone configuration (Figure 2), the Radio Link Module (RLM) will function as a relay RLM, that will forward the data communication from one computer to another within the same wireless cell.

This is the quickest and easiest way to set up a small wireless LAN infrastructure.

The mobile stations communicate via RLM.

Figure 2 Stand Alone Configuration



The wireless infrastructure is identified by a unique network name. All equipped devices that wish to connect to this network, must be configured with an identical network name.

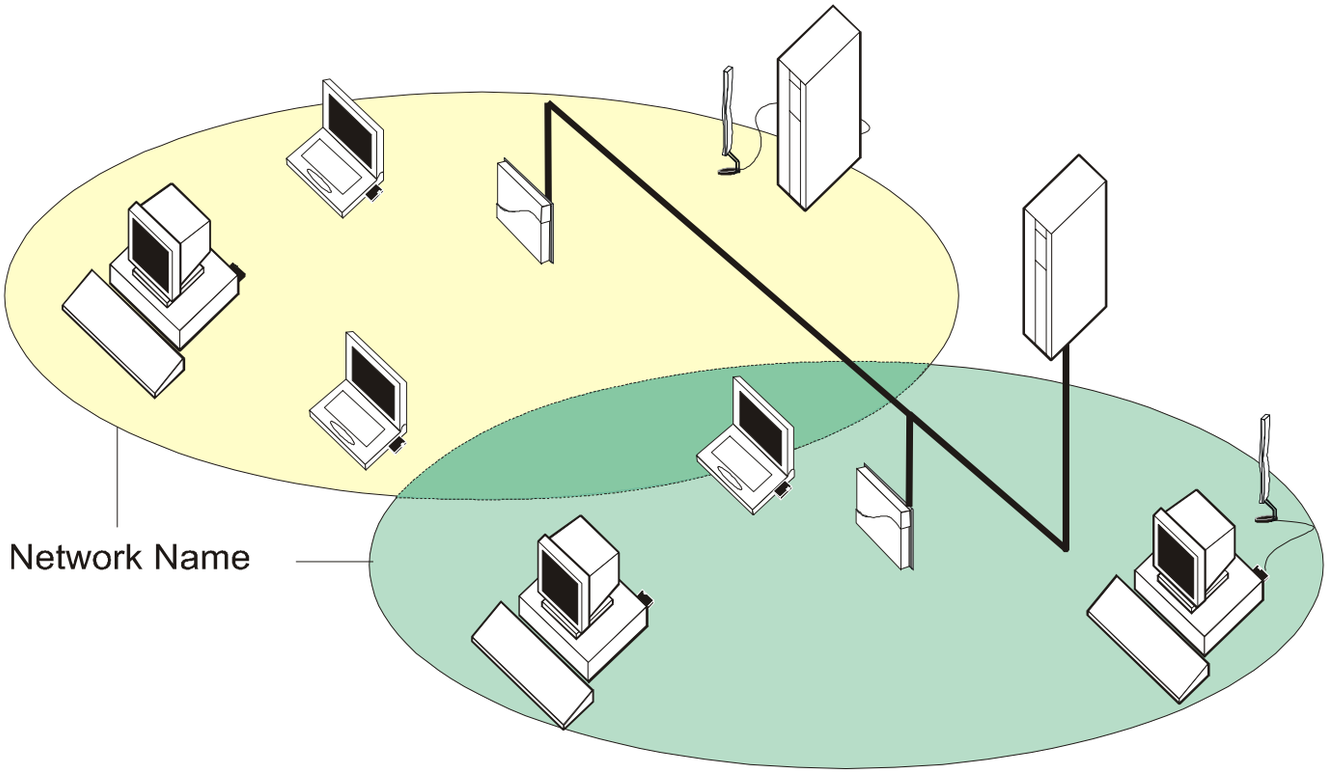
Mobile wireless stations will maintain communication with the infrastructure as long as they remain within range of the Access Point RLM.

2.3.2 Wireless Access to Ethernet Networks

Connecting Access Point RLM to an Ethernet network, as pictured in Figure 3 Wireless to Ethernet Access Configuration, allows you to:

- create a wireless environment for mobile computers, or
- connect a number of wireless stations to an existing Ethernet infrastructure, creating a larger coverage area.

Figure 3 Wireless to Ethernet Access Configuration



All wireless stations within this coverage area that wish to connect to the network must be configured with the same network name as the Access Point RLMs.

Roaming wireless stations will automatically switch between RLMs, when required, thus maintaining the wireless connection to the network.

2.4 Advanced Infrastructures

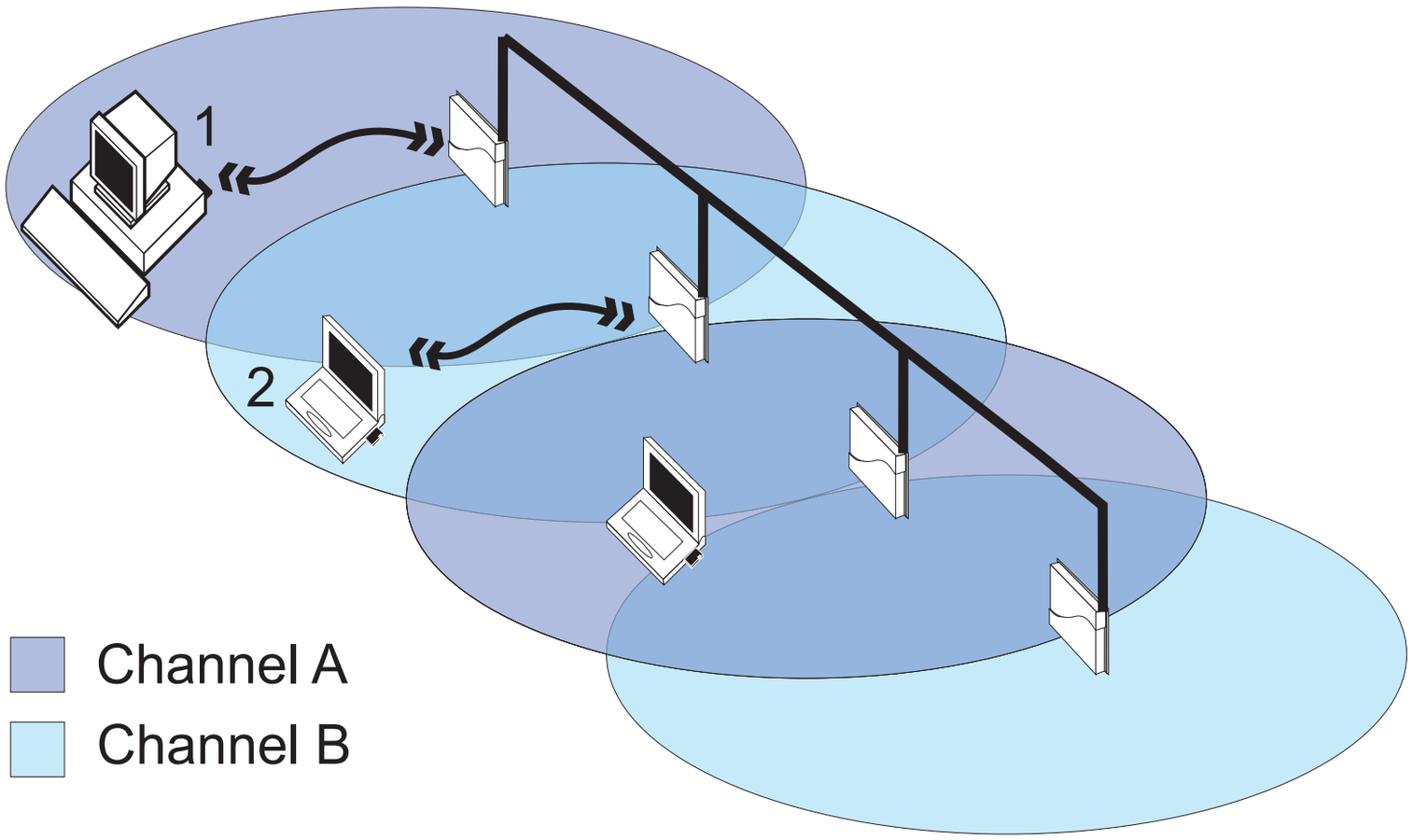
2.4.1 Multiple Channel Configuration

The stations are capable of switching their operating frequency channel dynamically when roaming between Access Points RLMs that have been configured to use different radio channels.

Using different channels enables you to optimize wireless performance, assigning different frequency channels to neighboring Access Points RLMs. Multiple frequency configurations may prove very useful in environments where:

- A high concentration of wireless stations are operational.
- The stations experience a performance decrease in terms of network response times as a result of the collision avoidance protocol (for more information, see “RTS/CTS Medium Reservation (page 131)”.

Figure 4 Dual Channel Configuration



- By configuring neighboring Access Points RLMs with different frequencies, you create separate mediums for each wireless cell. Operating at different channels, the stations can no longer “hear” one another, and therefore no longer need to defer communications.
- When the configuration pictured in Figure 4 Dual Channel Configuration represents a single channel system, both station 1 and station 2 share the same medium. Station 1 might need to defer communication with the Access Point RLM when it senses that station 2 is already communicating with the Access Point RLM in the neighboring cell.

As is the case in any roaming environment, you must configure all Access Points RLMs in multiple channel configurations with an identical network name.

The preferred channel separation between the channels in neighboring cells is 25 MHz (5 channels). Subject to the number of channels supported by the PC cards CP 1515 available in your country, this means that you can apply up to three different channels within your wireless network (see Table 2 Recommended Sub-Channel Configurations for recommended channel configurations).

Applying two channels that allow the maximum channel separation will decrease the amount of channel cross-talk, and provide a noticeable performance increase over networks with minimal channel separation.

To configure networks with multiple channels, refer to “Frequency Channel Management (page 138)” .

3 Setting Up your LAN Administrator Station

3.1 Introduction

SIMATIC NET Industrial Wireless LAN infrastructures are managed from the LAN administrator station. Within this chapter decision points are described which are necessary to help you set up LAN administrator station(s) to properly manage your network.

Typically, the LAN administrator station is a computer used by the LAN administrator to configure, manage and monitor the network. You can assign as many LAN administrator stations as you like, depending on how you would like to manage your network.

The LAN administrator station uses the tools available in the SIMATIC NET Industrial Wireless LAN software suite to configure and monitor your network. The following programs are included within the SIMATIC NET Industrial Wireless LAN software suite:

- CP 1515 Manager
- RLM Manager

In this chapter, we describe how to set up the LAN administrator station in the following network configurations:

- **Peer-to-Peer workgroup** - all stations within the network directly communicate with all other stations. No Access Points RLMs are necessary to bridge the data.
- **Infrastructure network** - all stations communicate to each other and the Ethernet backbone via Access Point RLM interfaces.

For an overview of the SIMATIC NET Industrial Wireless LAN software tools, please refer to "About Siemens SIMATIC NET Industrial Wireless LAN Tools" (page 17) .

3.2 Assigning an LAN Administrator Station

3.2.1 Minimum Requirements

To set up the LAN administrator station, you can use any desktop or portable computer that meets the following requirements:

- A Pentium II/266 Mhz or faster processor.
- Free disk space of 4 MB.
- 64 MB RAM (128 MB or more recommended).
- Microsoft Windows 98, ME, 2000 or NT 4.0.
- CD-ROM drive.

For the **CP 1515 Manager** you will also need:

- The PC cards CP 1515

For the **RLM Manager** you will need the following requirements:

- Access to the LAN, via
  1. PC card CP 1515
  2. Ethernet card
- SIMATIC NET Industrial Wireless LAN Access Point RLM.
- A installed TCP/IP protocol that provides a Windows sockets (winsock) interface. The TCP/IP drivers can be found on the Microsoft Windows installation disks or CD-ROM.
- CD-ROM drive.

NOTE:

For managing your wireless network you are adviced to set the IP-addresses of the RLM and mobile CP 1515 as described in "About IP Addresses and Subnets" (page 229).

3.3 Managing Peer-to-Peer Workgroups

A Peer-to-Peer workgroup consists of several stations communicating directly to each other without bridging data via the Access Point RLM.

Peer-to-Peer workgroups do not need the Siemens SIMATIC NET Industrial Wireless LAN tools. For more information refer to the “Industrial Ethernet Wireless LAN CP 1515” documentation that comes with your product.

3.4 Managing Infrastructure Networks

In an infrastructure network, you will primarily use the LAN administrator station that has the RLM Manager installed to configure your Access Points RLMs and monitor the radio traffic between selected Access Points RLMs and stations within the network.

You may also install the CP 1515 Manager on all stations within the network, or on selected mobile stations with the PC Card CP 1515, to monitor the link between the mobile station and the nearest Access Points RLMs.

3.4.1 Wired or Wireless?

The choice for a wireless or wired LAN administrator station will depend on your preferences and abilities to administer your network.

You should first determine how you would like to manage your network. If you like to configure and monitor stations from:

- **on-site**, to troubleshoot problems at the physical location of the station, you may choose to have a mobile, wireless LAN administrator station.

  Tool: RLM Manager and CP 1515 Manager
- **a central location**, such as the LAN administrator station, you may prefer a wired LAN administrator station.

  Tool: RLM Manager
- **a remote location**, via modem, calling into a RAS or PPP entry point to your network.

  Tool: RLM Manager

Your next consideration for wired or wireless station should be the size of your network. For instance:

- in larger networks, it may be more convenient to manage the stations from a central location, so a wired station would be more appropriate.
- in smaller network configurations, in which there are only few Access Points RLMs, a mobile, wireless station may be the most efficient way to configure and manage your network.

For wireless stations the following has to be considered:

- LAN administrators require easy access to wireless areas, e.g. for on-site troubleshooting.
- You need to do a site verification to determine optimal placement of Access Points RLMs.
- It is also possible remote configure and monitor the Access Point RLM via a dial-up connection. This feature is only possible when the network is externally accessible via a router.

Of course you can assign multiple stations as LAN administrator stations, allowing for a combination of wired and wireless stations and allowing you the freedom to choose the most appropriate tool for the situation.

3.4.1.1 Wired Stations

A wired LAN administrator station allows you to configure and monitor Access Points RLMs through a wired backbone by using the RLM Manager tool.

3.4.1.1.1 Configuration

A wired LAN administrator station has access to all Access Points RLMs via a wired backbone. The Access Points RLMs are identified by means of their unique IP address.

When your LAN architecture is comprised of multiple subnets, separated by gateways or routers, please note that the LAN administrator station which you intend to use for the initial configuration, must be on the same subnet as the Access Points RLMs.

Once the Access Points RLMs have been configured and their IP addresses have been registered, you can use any station to access the Access Points RLMs via the TCP/IP protocol.

For more information on configuring your Access Point RLM, please refer to "Configuration Scenarios" (page 47).

3.4.1.1.2 Monitoring

When you use a wired LAN administrator station you will not be able to move around to different physical locations of the network to determine or optimize the placement of stations or Access Points RLMs.

However, a wired LAN administrator station can use the RLM Manager remote link test and remote statistics features to do monitoring tasks.

With the RLM Manager you can validate radio frequency links between a remote Radio Link Module (RLM) and wireless stations connected to that Radio Link Module (RLM). For more information on monitoring, refer to "Monitoring Options" (page 98).

3.4.1.2 Wireless Stations

A wireless, mobile LAN administrator station allows you to use the CP 1515 Manager as well as the RLM Manager.

The Mobic uses only its CP 1515 Manager.

3.4.1.2.1 Monitoring

You can use the following tools to monitor your infrastructure network:

- CP 1515 Manager
  - PC card CP 1515 diagnostics
  - Logging measurements data
  - Site monitor
  - Link test
- RLM Manager
  - System information
  - Remote link test
  - Remote statistics

For more information on monitoring your network, refer to chapter 5 "Monitoring your SIMATIC NET IWL Network" (page 67).

3.5 Installing SIMATIC NET IWL Software

3.5.1 CP 1515 Manager

The CP 1515 Manager is a diagnostics tool that runs on wireless stations only. To setup the LAN administrator station that is capable of running the CP 1515 Manager program, the station must be equipped with the PC card CP 1515.

To install the CP 1515 Manager software, proceed as follows:

1. Insert the SIMATIC Wireless LAN software CD-ROM that came with your PC card CP 1515 into the station that you have designated as the LAN administrator station.

   If you downloaded the software from the web, please refer to the installation instructions found on the web.
2. When the CD Browser automatically starts you can proceed with the next step. If not:
   - Click the **Start** button on the Windows task bar, then select **Run**.
   - Click the **Browse** button in the Run window.
   - Select the drive letter of your CD-ROM player, then select the file "setup.exe" , and click the **Open** button.
   - Click the **OK** button in the Run window. The CD Browser will start-up.
3. Click on **Install** RLM**-,** CP 1515**-Manager**
4. Click on **Install** CP 1515 **Manager**.

5. Follow the instructions on your screen. If not available yet, a special Siemens group in the Windows Programs menu will be created. This group will provide access to the CP 1515 Manager.

NOTE:

Previously installed versions of the CP 1515 Manager program will automatically be replaced.

During the installation, you will be prompted for a directory to install the program files. The default directory for the CP 1515 Manager program is:

C:\Programs\Siemens I-Gate\Clientmanager

Throughout this manual, we make references to a variety of files. Unless otherwise specified, you will find these files in this default directory.

3.5.2 RLM Manager

The RLM Manager can be installed on both wireless and wired stations. To install the program, you will need to select a station that is configured with:

- Network Interface Card (NIC) to connect this station to the network. The NIC cards can be of any type, including:
  1. PC card CP 1515 (for wireless stations)
  2. Ethernet card
- TCP/IP protocol stack (see "Verifying the TCP/IP Protocol Settings" (page 43)).

3.5.3 Installing RLM Manager

To install the RLM Manager software, proceed as follows:

1. Insert the software CD-ROM that came with your product in the CD-ROM drive of the computer that you have designated as the LAN administrator station.

   If you downloaded the software from the web, please refer to the installation instructions found on the web.
2. When the CD Browser automatically starts you can proceed with the next step. If not:
   - Click the **Start** button on the Windows task bar, then select **Run**.
   - Click the **Browse** button in the Run window.
   - Select the drive letter of your CD-ROM player, then select the file "setup.exe" , and click the **Open** button.
   - Click the **OK** button in the Run window. The CD Browser will start-up.
3. Click on **Install** RLM**-,** CP 1515**-Manager**
4. Click on **Install RLM Manager**.
5. Follow the instructions on your screen. If not available yet, a special Siemens group in the Windows Programs menu will be created. This group will provide access to the RLM Manager software to configure your Access Point RLM.

NOTE:

Previously installed versions of the RLM Manager program will automatically be replaced, without affecting any other file that you might have saved into the program's directory. For example if you saved back-ups of Access Point RLM configuration files which you created with the previous version in the RLM Manager program folders, these files will not be deleted or overwritten.

During the installation, you will be prompted for a directory to install the program files. The default directory for the RLM Manager program is:

C:\Programs\ORiNOCO\AP Manager

Throughout this manual, we make references to a variety of files. Unless otherwise specified, you will find these files in this default directory.

3.5.3.1 Verifying the TCP/IP Protocol Settings

The RLM Manager program requires a TCP/IP networking protocol to communicate with the Access Point RLM. When setting up the Access Points RLMs for the first time you will need to verify the TCP/IP settings of the LAN administrator station and Access Point RLM.

You need an IP-address for your CP1515 in the LAN-admistrator station and an IP-address for the Access Point RLM.

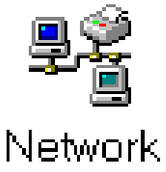
There are two ways to get the wright IP-address:

- the CP1515- or RLM IP-address is configured as "Obtain an IP address automatically" via DHCP. Your LAN admistrator has to configure the DHCP-server with the MAC-address of the CP1515 and RLM.

- you can set the IP-adresses manualy. You must order the korrect IP-adresses from your LAN admistrator (see also section "About IP Addresses and Subnets" (page 229)).

- When the network operating system in your network does not use the TCP/IP protocol, you will need to install it onto the LAN administrator station and assign a user-defined IP address to each LAN administrator station.
- When your network operating system uses the TCP/IP protocol, your station will already have an IP address assigned to it. This could either be a user-defined value, or a value assigned by for example a DHCP server. You do not need to modify this IP address.

To verify whether the TCP/IP protocol is properly installed, proceed as follows:



1. On the Windows task bar, click the Start button.
2. Point to **Settings** and then click on **Control Panel**.
3. In the Control Panel window, double-click the **Network** icon.
4. Verify that the list of network components includes the **TCP/IP Protocol** for the wireless network interface that you will use to access the Access Point RLM (e.g. your Ethernet or adapter).
   - If **Yes**, close all windows using the **Cancel** button and proceed with "Configuration Scenarios" (page 47).
   - If **No**, proceed as follows:
     a. Click the **Add** button.
     b. From the list of component types, select **Protocol** and click the **Add** button.
     c. Select the TCP/IP protocol from the list displayed.
     d. When your network does not use IP addressing, enable the option **Specify an IP Address**.

        This will disable the DHCP mechanism that would assign an IP address to your LAN administrator station automatically in networks that include a DHCP server.
     e. Enter a user-defined value in the **IP Address** field of the format **153.69.254.xxx**, where xxx may be any numerical value in the range of 1-253.

        When configuring multiple LAN administrator stations, make sure to assign different values to each station.

f. In the Subnet Mask field enter the value **255.255.255.0**

g. Click the **OK** button to confirm and follow the instructions as displayed on your screen.

5. When prompted to restart your computer, select **Yes**.

Once your computer has restarted, you will be ready to configure the Access Point RLM via any of the configuration scenarios as described on "Configuration Scenarios" (page 47).

3.6 Configuration Scenarios

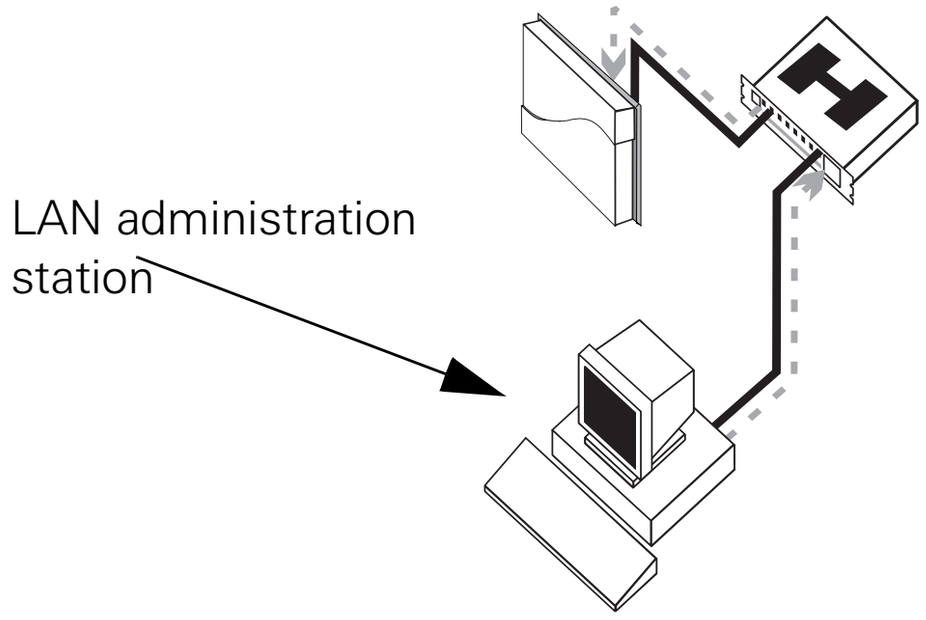
In the previous section you may have selected either a wired, or a wireless LAN administrator station. This section will describe some of the characteristics and features of each type and identify whether further modifications to the setup of your computer or “desktop workplace” are required.

3.6.1 Wired LAN Administrator Station

Using a wired LAN administrator station allows you to configure Access Points RLMs via:

- A “desktop workplace” setup, connecting your computer to the Access Point RLM via a hub or Ethernet switch as pictured in Figure 5 Wired Access via a Direct Cable Connection or direct via a TP cross-cable.
- A regular wired Ethernet connection as pictured in Figure 6 Wired Access via a Network Connection.

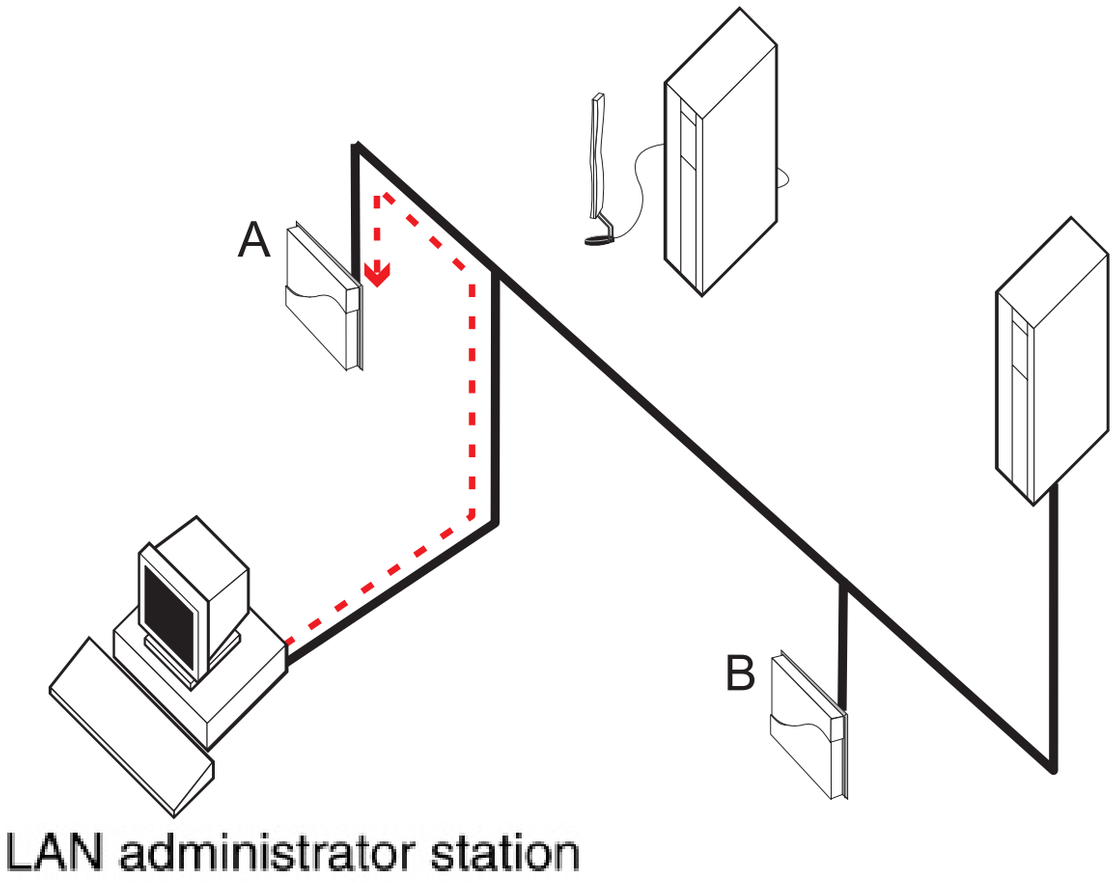
Figure 5 Wired Access via a Direct Cable Connection



Selecting a wired LAN administrator station is recommended in one of the following situations:

- You prefer to manage your Access Points RLMs from a fixed central location.
- The Access Points RLMs will be installed on remote locations, that are accessible via TCP/IP networking.

Figure 6 Wired Access via a Network Connection



Looking at Figure 6, the LAN administrator station has access to both Access Points RLMs **A** and **B** via the wired backbone.

- When these Access Points RLMs are still using the “out-of-the-box” configuration, the Radio Link Modules can be identified by means of their Ethernet MAC Address, provided that the Access Points RLMs are on the same subnet as your LAN administrator station (i.e. there are no routers between your LAN administrator station and the Access Point RLM).

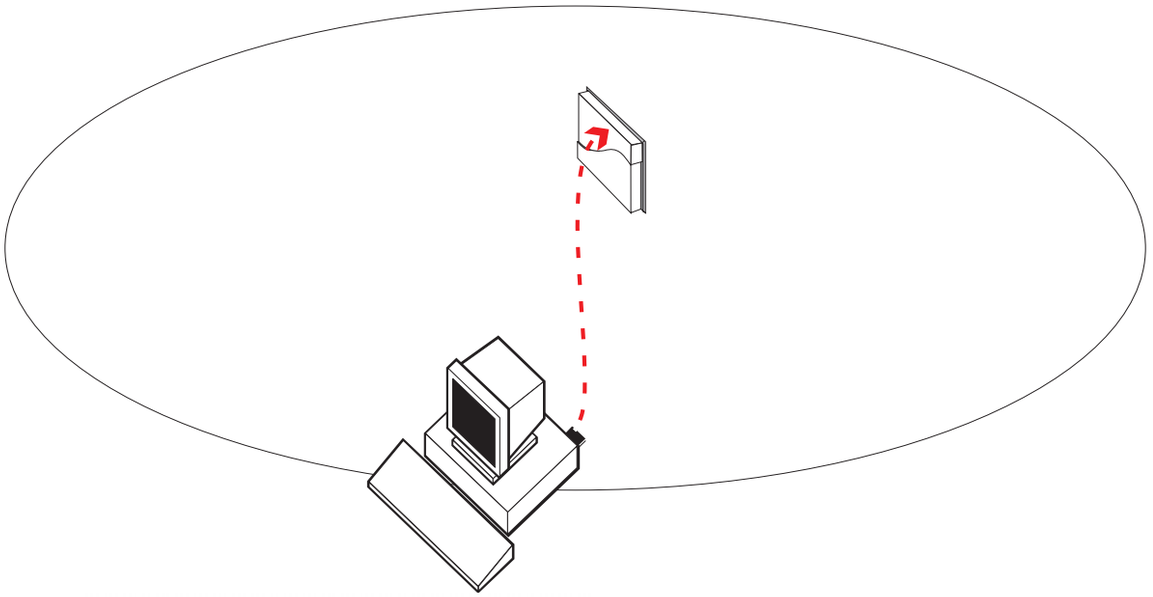
- When you have assigned a unique IP address value to each Access Point RLM, you should be able to access each Access Point RLM from anywhere within the network by using its unique IP address.

When installing new Access Points RLMs "out-of-the-box," you are advised to configure the Radio Link Modules one-by-one using the "desktop workplace" scenario as pictured in Figure 5 Wired Access via a Direct Cable Connection. This will allow you to assign a unique IP address value to each unit prior to connecting the units to the network infrastructure.

3.6.2 Wireless LAN Administrator Station

A wireless, mobile LAN administrator station allows you to use the RLM Manager in combination with the CP 1515 Manager tool.

Figure 7 Wireless Access via a Direct Connection



Using a wireless LAN administrator station allows you to configure Access Points RLMs:

- Directly by means of a wireless point-to-point connection as pictured in Figure 7 Wireless Access via a Direct Connection, or
- Indirectly by means of a wireless point-to-point connection with another Access Point RLM that provides access to the “target” Access Point RLM via a network backbone as pictured in Figure 8 Wireless Access via an Indirect Connection.

NOTE:

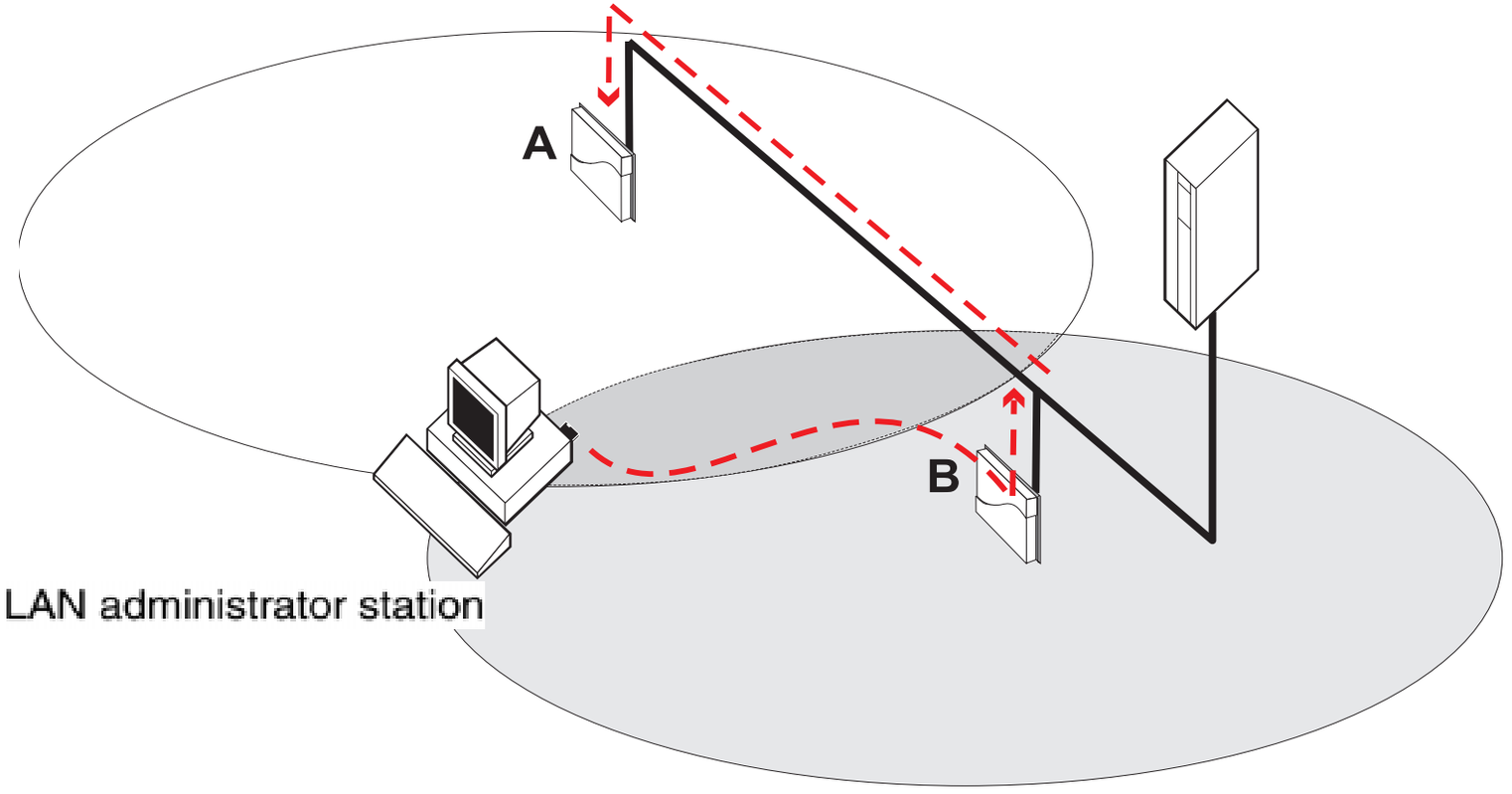
In the same manner in which wired networks require you to verify that all cables are connected properly to establish connection, wireless networks require you to verify that:

— the LAN administrator station is within range of the “target” Access Point RLM, and

— the wireless network interface setup matches the parameter values of the Access Point RLMs.

When using the configuration setup as pictured in Figure 7 Wireless Access via a Direct Connection, the wireless network interface of the LAN administrator station should be configured to match the settings of the “target” Access Point RLM.

Figure 8 Wireless Access via an Indirect Connection



When looking at the scenario pictured in Figure 8 Wireless Access via an Indirect Connection, the wireless network interface of the LAN administrator station should be configured to match the settings of Access Point RLM **B**.

- The scenario pictured in Figure 7 Wireless Access via a Direct Connection will be most convenient when configuring multiple “out-of-the-box” Access Points RLMs sequentially.
- The scenario pictured in Figure 8 Wireless Access via an Indirect Connection will be most efficient when adding new Access Points RLMs to an existing network or when you are not within range of the “target” Access Point RLM.

In both scenarios the Access Points RLMs are identified by means of their unique IP address.

3.7 Uninstalling SIMATIC NET IWL Software

If you wish to remove the SIMATIC NET Industrial Wireless LAN software from the LAN administrator station you can use the “Add/Remove” function of your Windows operating system.

To uninstall SIMATIC NET Industrial Wireless LAN software:

1. On the Windows taskbar, click the **Start** button.
2. Click on **Settings** and then **Control Panel**.
3. On the Control Panel window, double-click the **Add/Remove Programs** icon.
4. Select the program that you wish to uninstall, and click the **Add/Remove** button.

The **Add/Remove** option will remove program files only. If you have stored log files in the program files directory, these files will not be removed.

4 Basic Network Configuration

4.1 Introduction

This chapter will describe how to configure the SIMATIC NET Industrial Wireless LAN network for:

- Peer-to-Peer workgroups, and
- Infrastructure networks

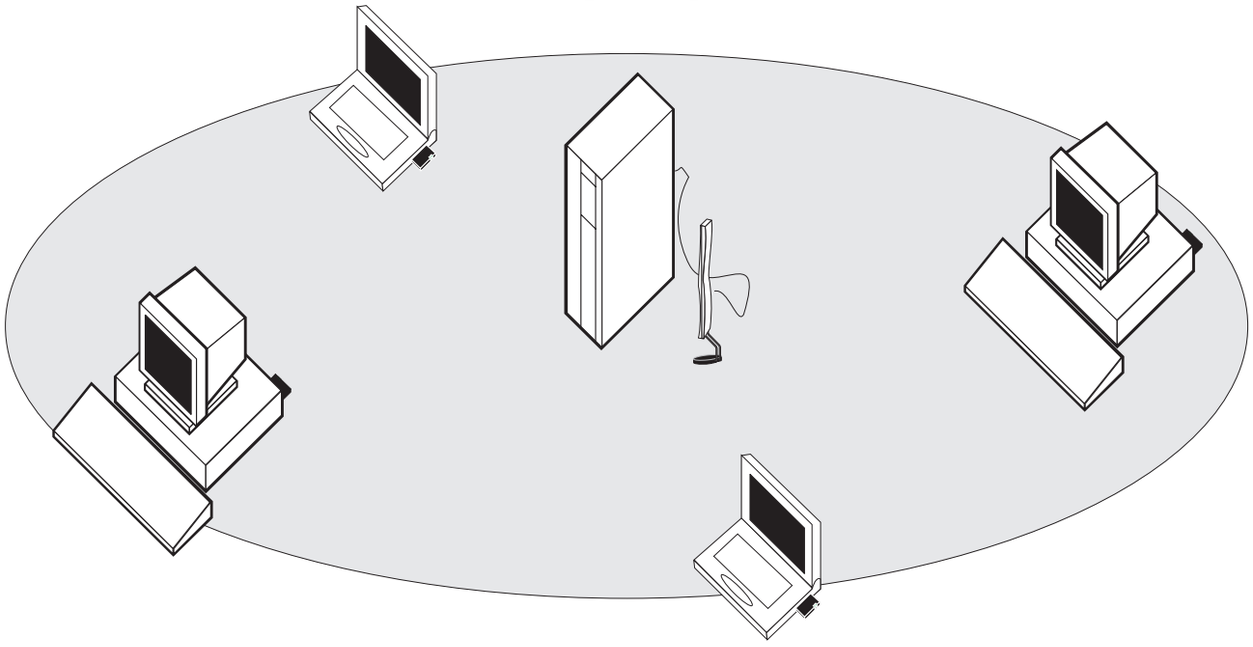
4.1.1 Peer-to-Peer Workgroups

A Peer-to-Peer workgroup consists of several wireless stations communicating directly with each other without bridging data via the RLM (see Figure 9 Peer-to-Peer workgroup).

To set up a Peer-to-Peer workgroup operating with the standard protocols, do the following:

- Set all stations to connect to a Peer-to-Peer workgroup.
- Set all stations to use the same Network Name.
- Set all stations to use an identical encryption key.

Figure 9 Peer-to-Peer workgroup



4.1.2 Infrastructure Networks

The number of network configurations that you could create using Access Points RLMs and SIMATIC NET Industrial Wireless LAN products is unlimited. Therefore, we have divided the rest of this chapter into three sections that should help you get your network up and running.

- The instructions for Configuring Infrastructure Networks (page 58) will work fine in most networking environments.
- More advanced configurations settings are described in chapter 8 Advanced Network Configurations (page 190).
- The Advanced Parameters (page 191) may help you with tailoring the Radio Link Module configuration to meet your networking requirements.
- Configuring Large Networks (page 218) provides a procedure to manage RLM devices more efficiently.

4.1.2.1 What you Need

To manage your Access Points RLMs, you must assign a unique IP address to each RLM within your network.

Furthermore, your management station must also have an IP address. The TCP/IP connection of your station should either:

- Be connected to the same subnet as the Access Points RLMs, as described in Basic Infrastructure (page 26), or
- Provide access to the subnet of the Access Points RLMs via routers, gateways or another type of LAN connection that supports the TCP/IP protocol.

4.2 Configuring Infrastructure Networks

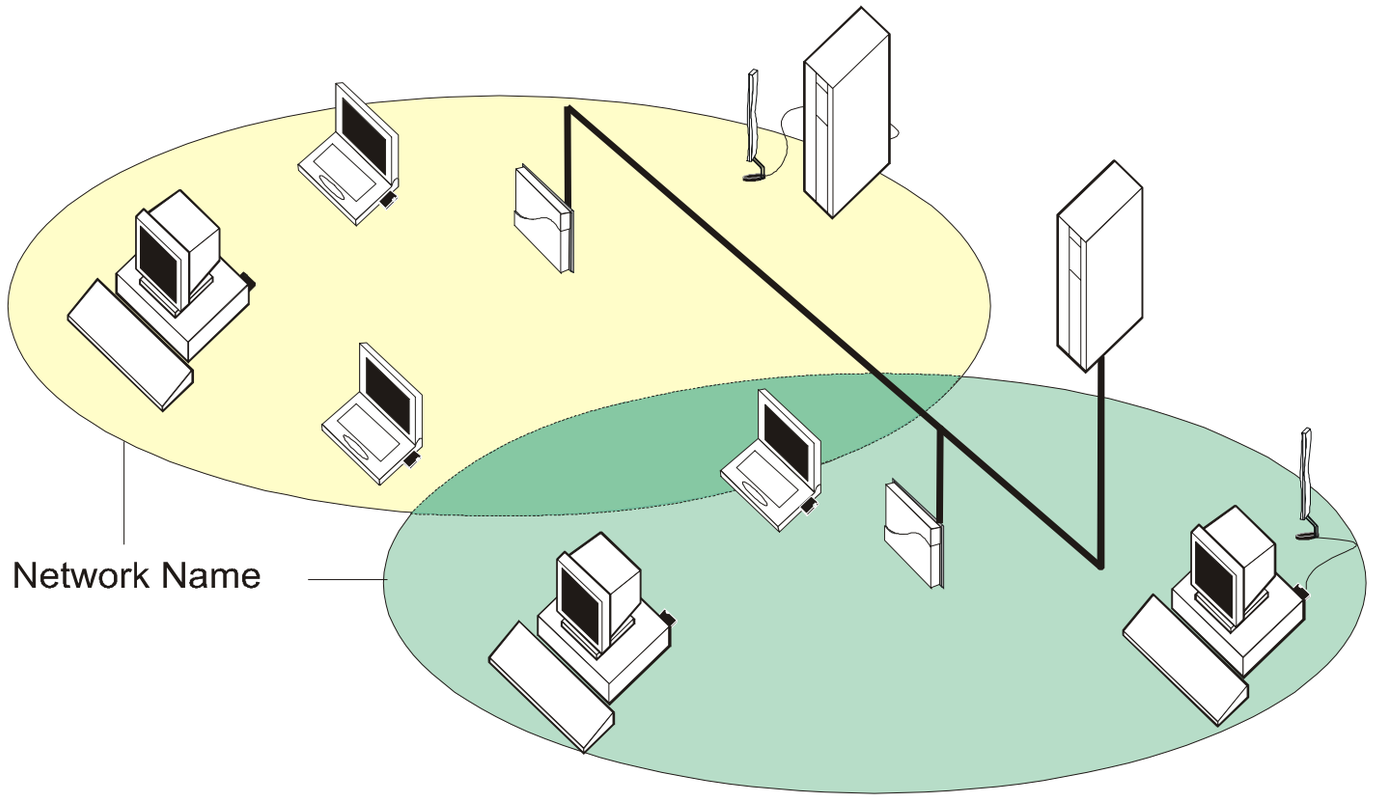
4.2.1 Basic Configuration

4.2.1.1 Introduction

This section will describe a 4-step installation approach to configure your Access Points RLMs to service a roaming network environment for (mobile) wireless stations.

Looking at the example pictured in Figure 10 Basic Access Network, each wireless cell is serviced by one RLM that has been set to “RLM Services”. All Access Points RLMs share the same Network Name.

Figure 10 Basic Access Network



To connect a wireless station to the SIMATIC NET Industrial Wireless LAN network, each station must be configured with the same Network Name as the Radio Link Module.

To configure the wireless stations, follow the instructions as described in the documentation that comes with your PC card CP 1515.

To install and configure the RLM perform the following steps:

1. Install the Radio Link Module hardware [1] .
2. Connect to the RLM with the RLM Manager program.
3. Set the Network Name and save configuration to the Radio Link Module.

1. Subject to the decisions you made in Setting Up your LAN Administrator Station (page 32), you may either install the Access Points RLMs at your desk and configure them one by one, or have the Access Points RLMs mounted directly in their various locations prior to configuring them via a network connection.

4. Create a back-up file of the new configuration settings (optional but recommended).

Repeat steps 2 to 4 for each of the Access Points RLMs that you wish to install.

4.2.1.2 Step 1 - Installing the Access Point RLM

For installation instructions of the RLM hardware, please refer to the documentation that was includeded with the RLM.

4.2.1.3 Step 2 - Connecting to the Access Point RLM

To connect to the Radio Link Module, you need to address each Radio Link Module via its IP address.

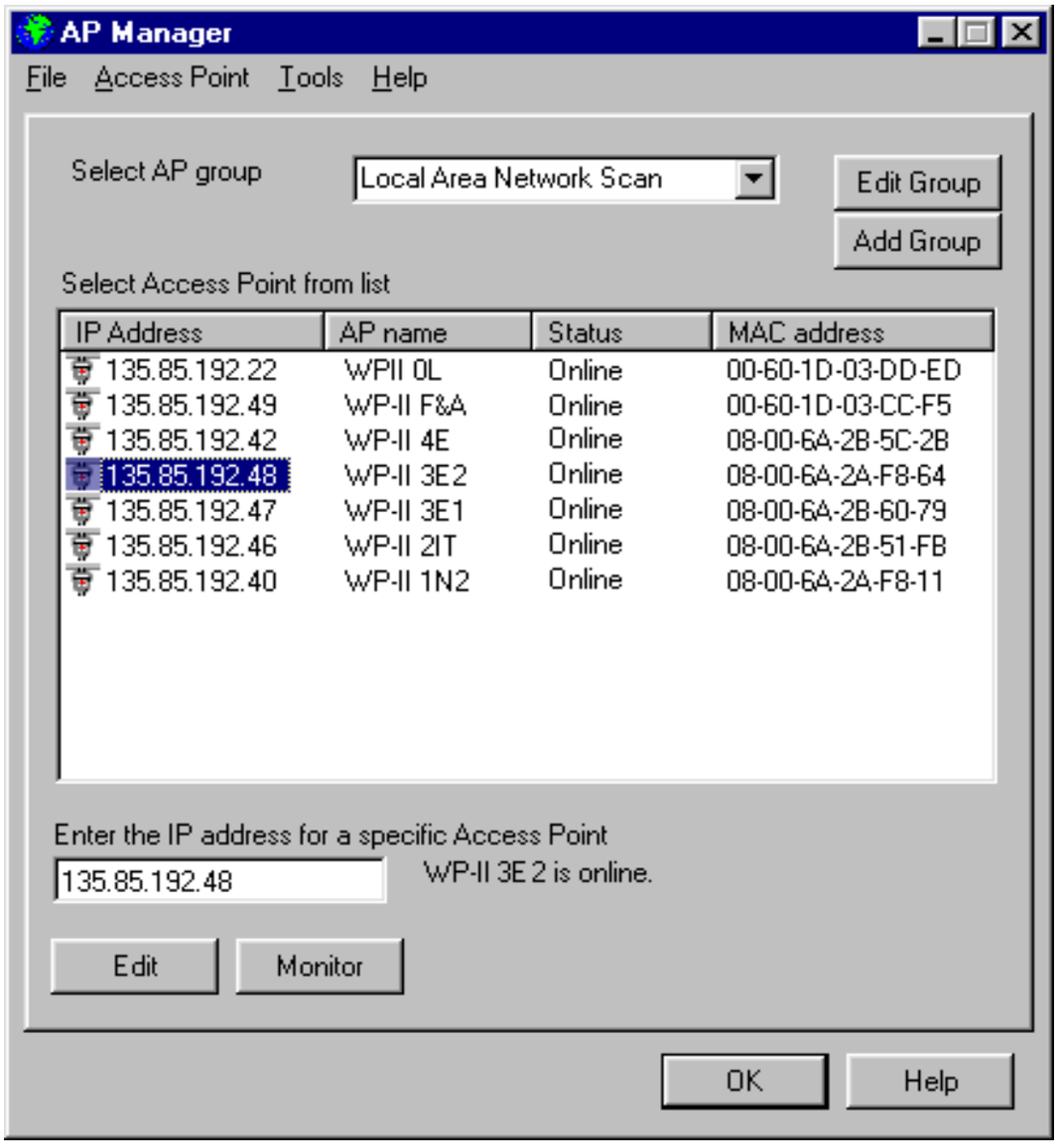
- If your network includes a BOOTP or DHCP server, the IP address will be assigned automatically (refer to BOOTP and DHCP (page 231) for more information about BOOTP/DHCP).
- In situations where no IP addresses are assigned automatically, the LM factory default IP address will be 153.69.254.254.

  You must change this factory-set IP address (153.69.254.254) upon first configuration.

To connect to the RLM proceed as follows:

1. Start the RLM Manager program.
2. Select the Radio Link Module that you wish to configure from the list or enter the IP address in the field **Enter the IP address for a specific** RLM (see Figure 11 Main RLM Manager window).
   - A new Radio Link Module is marked with a special icon.
   - This list will display all Access Points RLMs located on the same IP subnet as your management station (see also Modifying the Configuration (page 226)).
   - To gain access to Access Points RLMs on a different subnet or via a dial-up connection, enter a specific IP address in the field **Enter the IP address for a specific** Access Point RLM.

Figure 11 Main RLM Manager window



3. Click the **Edit** button.
   - If the RLM that you select is identified by the factory-set IP address 153.69.254.254, you will be prompted to change this IP address.
     a. Enter a unique IP address for the Radio Link Module in the field access point **IP Address**.

b. Record the IP address on the **RLM Configuration Record** located in A "Start-up Configuration".

4. Enter the Read Write password and click **OK** (default password is "public").
   - If the RLM is found and if you entered the right passwords, a new window appears with parameter tabs to change the configuration (see Figure 12 RLM Manager Wireless Interfaces tab).
   - If the Radio Link Module is not found in the network and/or the configuration is not read, or if the wrong password is entered, the message "**Invalid password**" appears.
     Click **OK** to return to the main RLM Manager window and try again.

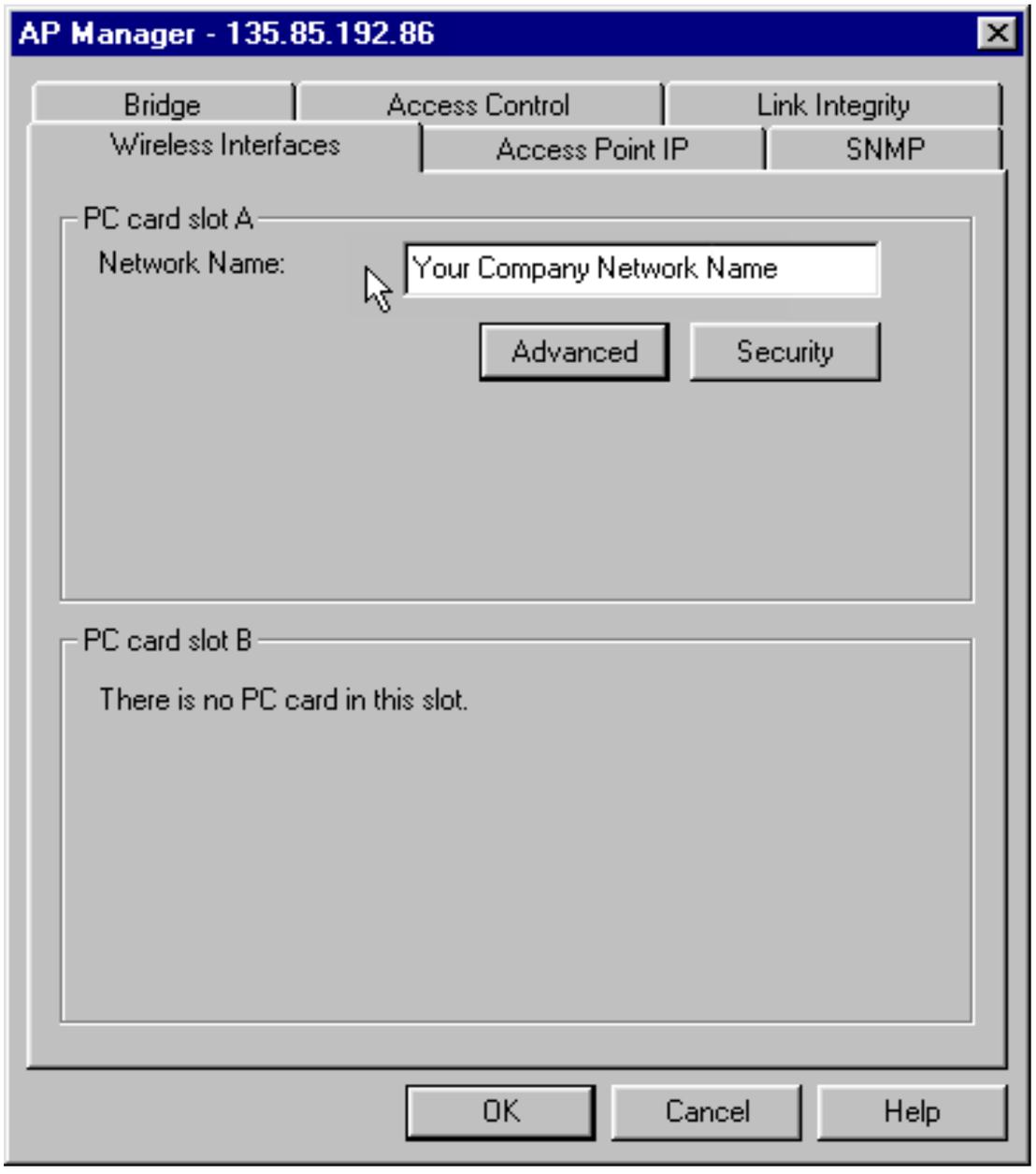
You are now ready to change the RLM configuration settings.

4.2.1.4 Step 3 - Set Network Name and Save Configuration

When installing the SIMATIC NET Industrial Wireless LAN network, you are advised to modify the default settings of the wireless network interfaces. Although the Radio Link Module will work fine with its factory-set values, changing the parameters to unique values will differentiate your network from possible neighboring networks.

1. Select the tab **Wireless Interfaces** (see Figure 12 RLM Manager Wireless Interfaces tab).
2. Choose the slot of the RLM (**PC Card slot A** or **B**) that contains the PC Card that you wish to configure.

Figure 12 RLM Manager Wireless Interfaces tab



3. Enter the identification designator in the field **Network Name** for the service type that this interface should use:

   The network name can be any alphanumeric string from 1 to 32 characters in the range of “a” to “z,” “A” to “Z” and “0” to “9.”

The network name should be the same for all wireless network interfaces that will service wireless stations that belong to the network.

The network name distinguishes your Access Points RLMs from Access Points RLMs that belong to a neighboring network.

For information on other Interface parameters (like the **Advanced** and **Security** button), see Advanced Network Configurations (page 190).

4. When finished changing parameters, click **OK** to save the configuration to the Access Point RLM and to return to the main RLM Manager window (as pictured in Figure 11 Main RLM Manager window).

   At this stage, the IP address and other settings are stored in the volatile memory of the RLM.

WARNING:

If you save the configuration to the Radio Link Module (by clicking the OK button), the RLM reboots automatically.

This will complete the basic configuration of your RLM. This basic configuration will work efficiently in most networking situations. You are advised to make a back-up file of this configuration as described in Step 4 - Create a Back-up of the Configuration (page 66).

More advanced parameter settings are discussed in Advanced Network Configurations (page 190).

4.2.1.5 Step 4 - Create a Back-up of the Configuration

At all times when you change the configuration of the Access Point RLM, we recommend that you create a back-up file of the configuration. You can use this back-up to quickly restore the Radio Link Module configuration in situations where:

- Your Access Point RLM goes out of service.
- You would like to recreate the original configuration of the RLM that you had to replace (for example following a repair).
- When you need to perform a forced reload as described in Forced Reload Procedure (page 244).

To create a back-up file proceed as follows:

1. Start the RLM Manager program.
2. Select the RLM you want to create a backup of.
3. From the Radio Link Module menu select **Download Config File**.
4. When prompted for a name, enter a name that allows you to easily recognize the relationship between the file name and the Radio Link Module.
5. Record the filename and the location where the RLM will be installed on the “Access Point RLM Configuration Record” in table Access Point Configuration Record (page 235).

To install and configure other Access Points RLMs, refer back to Step 1 - Installing the Access Point RLM (page 60).

5 Monitoring your SIMATIC NET IWL Network

5.1 Introduction

Once your network has been configured and installed, you can use SIMATIC NET IWL software tools to:

- Monitor the performance of your network;
- Verify optimal placement of your Access Points RLMs and wireless stations.

You are advised to verify the performance of your network on a regular basis, as performance may change when wireless stations are relocated, or office environments add or re-arrange cube walls, or when new equipment is installed that might interfere with the wireless communication.

5.1.1 SIMATIC NET IWL Tools

The SIMATIC NET IWL software suite offers two tools that enable you to monitor your network:

- CP 1515 Manager
- RLM Manager

5.1.1.1 CP 1515 Manager

The CP 1515 Manager has been designed to monitor the radio performance of your network on-site. You can use this program to:

- Run dynamic radio communication diagnostics with the Radio Link Module within range of your monitoring station.
- Display detailed link test measurement results with the Access Point RLM nearest your CP 1515 Manager station.

The CP 1515 Manager is a mobile wireless tool that can only run on a wireless station (typically a portable device such as a notebook computer).

5.1.1.2 RLM Manager

The RLM Manager has been designed to monitor your network from a central location, e.g. the LAN administrator station.
You can use this tool to display link test measurements between a (remote) RLM of your choice and a station connected to the selected RLM.

The RLM Manager tool can run on both wired stations (Ethernet) and wireless stations. To run diagnostic measurements, the LAN administrator station must be connected to the network infrastructure that allows the station to access the Access Point RLM using the TCP/IP protocol.

5.1.2 Which Tool Should You Use?

The decision whether to use the CP 1515 Manager or RLM Manager largely depends on your capabilities or desire to do diagnostic measurements on-site, or from a central location.

Both the CP 1515 Manager and the RLM Manager offer logging functions that can save measurement data for later evaluation or comparison with previous measurements. You can view saved log files with any ASCII editor, or import the data into standard spreadsheet or database applications.

NOTE:

Alternatively you may use the RLM Manager program to monitor wireless performance of both wireless systems via Radio Link Modules (see Remote Link Test Window (page 103)).

The SIMATIC NET IWL products have been designed to be interchangeable with all other wireless LAN products that use the direct sequence radio technology, as identified in the IEEE 802.11 standard for wireless LANs. Operating in the unlicensed 2.4 GHz band, the SIMATIC NET IWL system can transmit through walls and floors, giving you the freedom to roam throughout the network while maintaining your network connection.

This means that your SIMATIC NET IWL hardware will communicate with other vendors' IEEE 802.11 compliant wireless LAN products.

However, you may not always be able to use the SIMATIC NET IWL software suite in combination with other vendors' products, due to the following reasons:

- The IEEE 802.11 standard for wireless LANs does not identify standards for diagnostic or management tools; i.e. each vendor may have designed a customized tool to configure and/or manage the IEEE 802.11 wireless network.

- The Siemens SIMATIC NET IWL software suite has been designed to offer an enhanced set of tools to monitor and analyze a wide range of diagnostic tallies.

  Some of these tools require additional functions in the hardware that (by default) is supported by all Siemens SIMATIC NET IWL products, but may not be supported by the other vendors' products.

If other vendors' products do not let you display the communications quality or configuration parameters using the SIMATIC NET IWL software suite, please refer to the documentation that was shipped with the other vendors' product.

5.2 Using the CP 1515 Manager

5.2.1 Monitoring Methods

The CP 1515 Manager offers four monitoring methods:

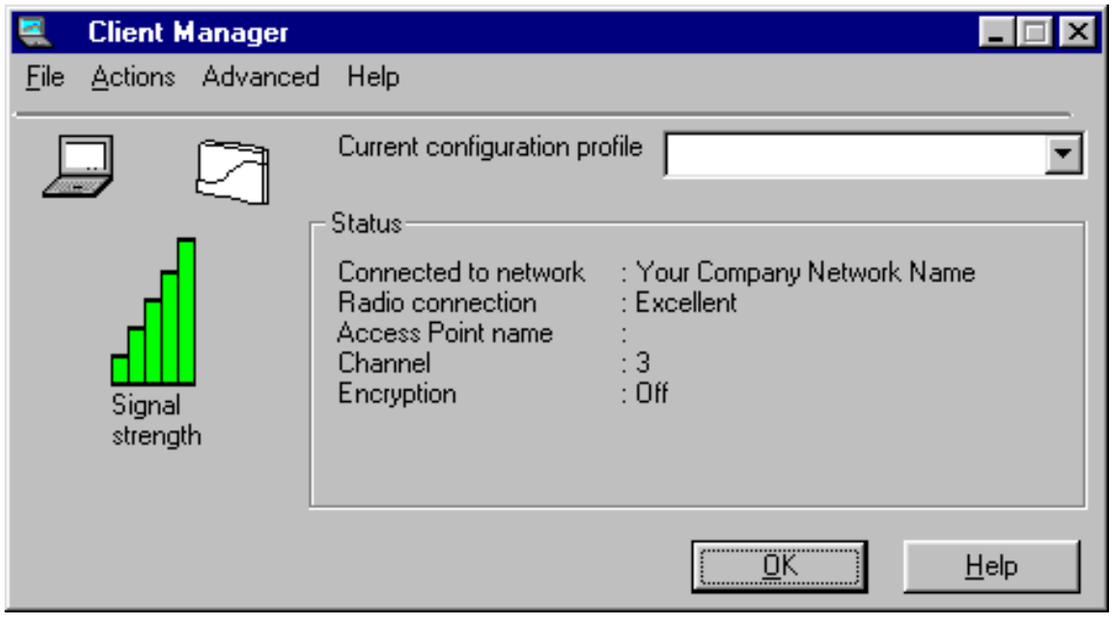
- PC Card CP 1515 diagnostics (see Diagnose Card (page 96))
- Link test (see Link Test Window (page 74))
- Site monitor (see Site Monitor Window (page 81))
- Logging measurement data (see Logging Measurement Data (page 92))

The site monitor, link test and logging measurement data options are only available when the CP 1515 Manager is installed in "Advanced" mode (see CP 1515 Manager (page 19))" for more information).

To start the CP 1515 Manager tool:

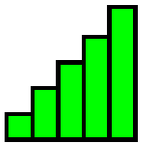
1. The CP 1515 Manager program starts automatically when Windows is started. The CP 1515 Manager icon is displayed on the windows task bar. If the program is not running:
   - Select the **Start** button on the windows task bar.
   - Select **Programs**, and click the **Siemens I-GATE** program group
   - Next select **Client Manager** to start the CP 1515 Manager program.
2. Click on the CP 1515 Manager icon in the taskbar to open the main CP 1515 Manager window pictured in Figure 13 Main CP 1515 Manager Window.

Figure 13 Main CP 1515 Manager Window



The main CP 1515 Manager window will display the key information required to validate the current network connection of your SIMATIC NET IWL station:

- The name of the network to which your station is connected ("Peer-to-Peer" in case of a Peer-to-Peer workgroup, or the network name of your RLM infrastructure, e.g. "Your company network name").
- The quality of the radio connection to this network:
  - Excellent
  - Good
  - Marginal
  - Poor, or
  - Out of range



The quality of the radio connection is also displayed with a colored icon. The color indicates the quality of the connection

- Green: Excellent or good connection
- Yellow: Marginal connection
- Red: Poor connection
- Red with error sign: No connection

- The name of the Radio Link Module to which the mobile wireless computer is connected at that moment.
- The channel used for the connection.
- Encryption: on / off

If your CP 1515 Manager could not establish a network connection, this screen will display either:

- **No wireless network card driver present** - your station was unable to detect the SIMATIC NET IWL driver. Check to make sure that the PC card CP 1515 is properly connected and that you have configured your station correctly.
- **Out of range** - you are out of range of the network for which your station has been configured.
- **Searching for initial connection to network: Network Name** - the network named Network Name can not be found.

For more detailed information use the monitoring methods as described in Monitoring Methods (page 71).

From the main CP 1515 Manager window (as pictured in Figure 13 Main CP 1515 Manager Window) you will also have access to a number of menu items. These menus are described in the next paragraphs.

If you are having problems connecting to the network:

- Click the **Help** button or press F1 for troubleshooting hints
- Refer to B "Troubleshooting" for possible solutions.

5.2.2 Link Test Window

You can use the link test mode to do detailed diagnostic measurements in indoor wireless environments between your CP 1515 Manager station and one specific test partner. Subject to the type of wireless network to which your CP 1515 Manager station is connected, the test partner may be either one of the following:

- The RLM, when your CP 1515 Manager station is connected to an "Infrastructure Network" (see chapter 2 Wireless Configurations).

  In this type of network you will not be able to select another link test partner; when roaming throughout the wireless network environment, the link test partner may change dynamically whenever another RLM provides better communications quality.
- The wireless station, when your CP 1515 Manager station is connected to a Peer-to-Peer workgroup (see chapter 2 Wireless Configurations).

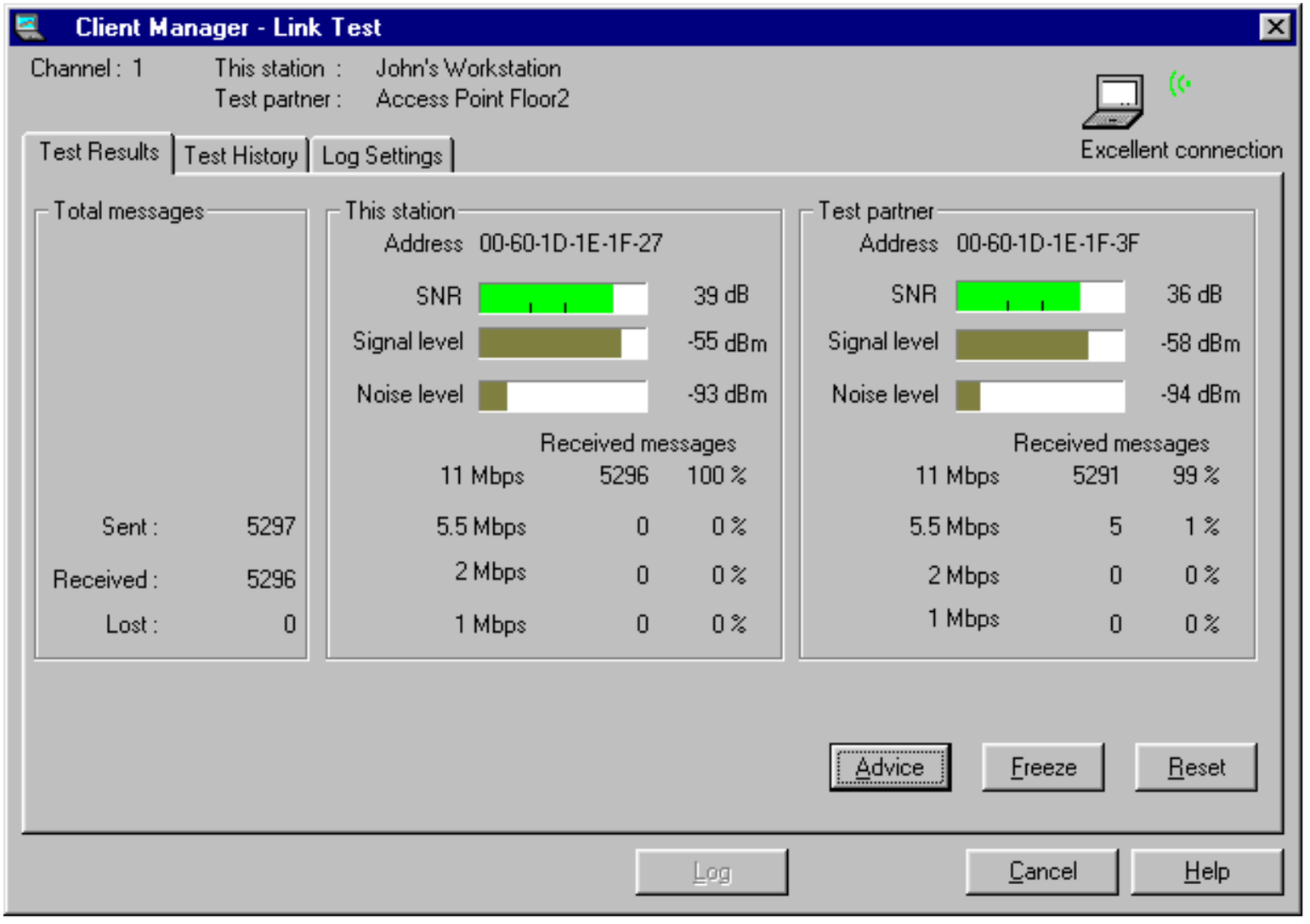
  In this type of network you will be able to select your link test partner from a list of stations available in the independent network identified by the same wireless network name as your CP 1515 Manager station.

To start the link test, select **Link Test** in the **Advanced** menu of the main CP 1515 Manager window. This will display the window pictured in Figure 14 Link Test Window.

Across the top of the Link Test window, you can see:

- The radio channel on which both devices are communicating.
- The name of your computer (This Station),
- The name of the link test partner (Test Partner), and
- The quality of the connection.

Figure 14 Link Test Window



The “Link Test” window provides you with three link test options to assist you in analyzing the link test data:

- **Test results** - provides measurement results of the link test.
- **Test history** - provides graphical results of the link quality.
- **Log Settings** - set the measurement parameters to record test results for future analysis.

5.2.2.1 Test Results Tab

The Test Results tab is your primary screen to analyze link test results using the following indicators:

- Signal to noise radio (SNR)
- Received messages

5.2.2.1.1 Signal to Noise Ratio (SNR)

The signal to noise ratio (SNR) identifies the communications quality of radio path between your station and the link test partner. This indicator is updated dynamically according to the actual status of the radio link.

The color of SNR indicator relates to the following levels of communications quality.

Color	Description
• Green	Communication quality is "Excellent" or "Good", no intervention is required.
• Yellow	Communication quality is "Marginal", no intervention is required.
• Red	Communication quality is "Poor", intervention required. (see chapter B Troubleshooting).

If the level of SNR is lower than expected the signal level and noise level indicators may help you investigate the cause:

- A low signal level indicates that the "strength" of the radio signal is fairly low: i.e. your SIMATIC NET IWL CP 1515 Manager station is almost 'out-of-range' of its link test partner.

- A high noise level indicates a source of radio interference in the radio path between the two link test partners.

  Comparing the values for your station and the link test partner will help you to identify the location where the interference occurs, and investigate whether any actions to eliminate or remedy the source interference resulted in a better performance.

5.2.2.1.2 Received Messages

The indicator "Received Messages" provides a way to determine the efficiency of the radio path between your CP 1515 Manager station and the link test partner.

When running a link test, your SIMATIC NET IWL CP 1515 Manager station will exchange messages with its test partner. The test partner will confirm proper receipt by returning an acknowledgment response.

Both your wireless station and the link test partner will use these messages to:

- Measure the signal to noise ratio (SNR).
- Compare the total number of messages sent to the number of messages received.
  - — When the communications quality is rated as "Excellent" or "Good," the total number of lost messages should be zero.
  - — When communications quality is "Marginal," the total number of lost messages may be in the range of 1% to 3%
  - — When the total number of messages is >5% your network environment will most likely suffer from performance problems.

In most situations you will see that the number of lost messages will increase whenever the level of SNR decreases.

The different fields for messages received at the different transmit rates (e.g. “11 Mbit/s”, “5.5 Mbit/s”, “2 Mbit/s” and “1 Mbit/s”) may serve as an indicator for network throughput efficiency.

It is normal behavior for SIMATIC NET IWL stations to retransmit messages that were lost (either as a result of a frame-collision, or because the test partner was “out-of-range”):

- If a message transmission fails, your wireless station will retransmit the “lost” frame.
- If re-transmitting fails repeatedly, the station will switch to a lower data speed[1] and try to transmit the message again.

The higher the number of messages received with the highest transmit rate, the better your throughput efficiency. A relatively high number of messages received at lower transmit rates may indicate:

- Inadequate radio performance, which can typically be related to the level of SNR, or
- Network congestion. This may typically be the case when the SNR was rated “Good”.

In situations where you see a lot of (re)transmissions at lower data rates, the lower data speed might be the result of:

- A link test partner that is almost “out-of-range” of your CP 1515 Manager station. This is easily recognized by a low level of SNR.

1. The range of wireless data is related to the data speed. Radio messages transmitted at lower data speeds will travel longer distances than messages at maximum data speed. In most network environments, the “Auto Fall-back” transmit rate will yield the best performance results.

- One of the test partners is using a wireless card that does not support the high rates.

To investigate link quality results in more detail, you can use one of the following buttons:

- **Advice** - to display more detailed information related to the current link quality and troubleshooting hints to increase performance.
- **Freeze** - to momentarily stop the dynamic indicators and updating of numerical values, for example to analyze the results on your screen in more detail.
- **Reset** - to reset all of the diagnostic counters back to zero.

  You can use this option to investigate the results of an action to remedy a cause of poor performance. For example after you switched off a microwave oven that you suspect is causing interference. Clicking the **Reset** button will analyze the link quality again, ignoring previous results that may have adversely influenced the statistics.
- **Help** - to display general information about the CP 1515 Manager link test.

  To access the on-line help system you can also press the F1 function key on your keyboard.

5.2.2.2 Test History Tab

You can use the Test History tab to display link test results as a line-chart. You can change the display to include the diagnostic parameters of your choice, and a user-defined time window. You can set the time window to display the information of the last minute, last hour or last 24 hours.

For example, if you have an Radio Link Module that shows mysterious performance problems at regular intervals, you can run the test history mode for 24 hours to:

- Determine the exact time the problem occurs in the selected Time window
- Analyze what was causing the performance problem without having to watch the dynamic indicators continuously.

5.2.2.3 Log Settings Tab

You can record the link test measurements to a log file, and use this log file to more fully analyze the link quality. The measurement data can be logged automatically at regular intervals or manually upon user-command.

For more information on log files, see Logging Measurement Data (page 92).

5.2.3 Site Monitor Window

The Site Monitor option enables you to display the communications quality between your CP 1515 Manager station and all Access Points RLMs within its range.

The site monitor has been designed for indoor roaming environments to:

- Determine the overall wireless coverage of your SIMATIC NET IWL network.
- Verify or optimize the placement of your Radio Link Modules, in order to provide seamless roaming connectivity to mobile stations.

When roaming throughout a wireless network environment with your CP 1515 Manager station, you will be able to identify areas that may not have adequate coverage, or that suffer from in-band interference from other (wireless) equipment such as security gates, microwave ovens or photo copiers.

To start the site monitor, select **Site Monitor** in the **Advanced** menu in the main CP 1515 Manager window. This will display the window pictured in Figure 15 Site Monitor window.

5.2.3.1 Options in the Site Monitor Window

- **Site Monitor** tab - the primary tab to monitor the performance of your wireless network (see Site Monitor Tab (page 83)).
- **Selection** tab - enables you to scan for neighboring SIMATIC NET IWL networks and select such networks for monitoring (see Selection Tab (page 86)).
- **Log Settings** tab - allows you to enable, disable or configure the site monitor logging options (see Logging Measurement Data (page 92)).
- **AP names** tab - allows you to create user-defined Access Point RLM names for easy identification of Access Points RLMs in the Site Monitor window (see AP Names Tab (page 90)).

NOTE:

The Site Monitor option only works in combination with Access Points RLMs. When you select this option in a Peer-to-Peer workgroup environment[1], the Site Monitor window will not start

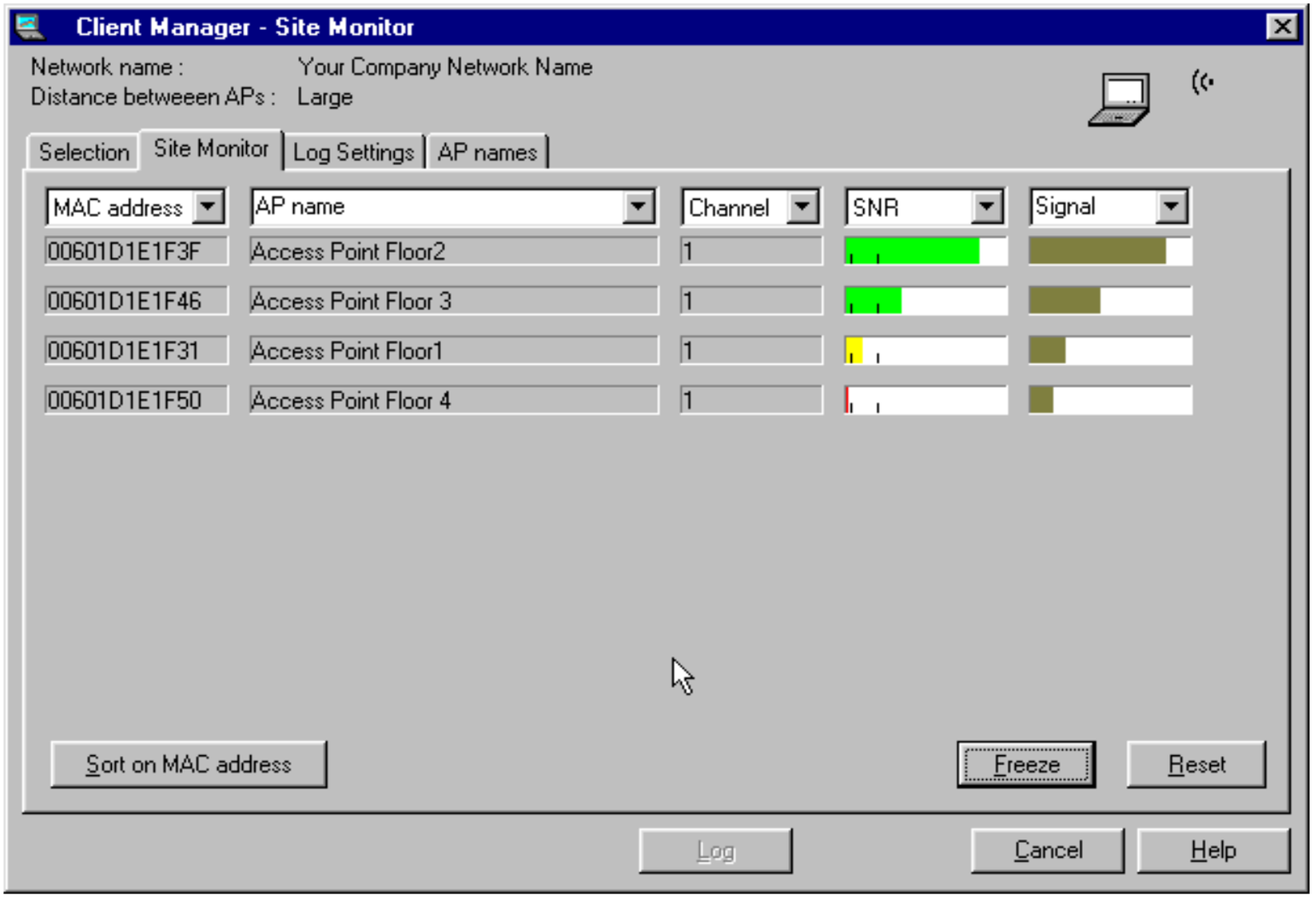
1. Independent networks never include Access Points RLMs (see also chapter 2 Wireless Configurations)

with the Site Monitor tab but will start with the Selection tab described on Selection Tab (page 86).

5.2.3.2 Site Monitor Tab

When you open the Site Monitor window, this will display the window pictured in Figure 15 Site Monitor window.

Figure 15 Site Monitor window



Displayed across the top of the Site Monitor window are the following fields:

- **Current Network (SSID)** - which identifies the name of the network to which you are currently connected.
- **Distance between APs** - describes the RLM density setting of the network to which you are currently connected.

These fields will remain visible when selecting any of the other options in the Site Monitor window.

Also displayed in the Site Monitor window are all Access Points RLMs that:

- Belong to the same Infrastructure as the one to which you are currently connected, and
- Are within range of your CP 1515 Manager station.

In the site monitor mode you can customize the selection of site monitor parameters to satisfy your personal preferences as described on Customizing the Site Monitor Display (page 85). The recommended selection for standard site survey procedures is as follows:

- **AP name** (RLM name) - to identify devices by the name of the RLM:

  This name is identified either in:

  — The **System Name** field of the RLMs configuration (see SNMP Parameters (page 211)).

  — A user-defined Access Point (RLM) **Name List**, that you can create using the CP 1515 Manager tool (see AP Names Tab (page 90)).
- **SNR** - the signal to noise ratio which indicates the communications quality with the various Access Points RLMs.
- **Channel** - to identify which radio channel is used by each of the Access Points RLMs.

To perform a standard site survey:

1. Arrange the site monitor display as described above.
2. Determine which locations in your network environment require wireless connectivity.
3. Use a mobile computing device to walk through your wireless LAN environment.
4. Roaming throughout the network environment, verify that each location is covered by at least one RLM that provides a level of SNR that is at least "Marginal" (Yellow) or better.
5. (optional) Use the **Sort on** button to re-arrange the display of Access Points RLMs by the data displayed in the first column.

   The first time you open the Site Monitor window, the Access Points RLMs are sorted in descending order of the SNR values.
6. (optional) To sort Access Points RLMs in a different way, simply select another display item in column one.

5.2.3.3 Customizing the Site Monitor Display

For specific purposes, you may wish to select one or more of the other parameters as well, for example:

- Display the signal level (**Signal**) and noise level (**Noise**) to determine the cause of a poor level of SNR.
  - A low signal level would indicate a "weak" radio signal, i.e. the Radio Link Module is almost 'out-of-range'.

— A high noise level would indicate a source of interference in the radio path between your CP 1515 Manager station and the Access Point RLM.

The SNR, signal level and noise level can be displayed as dynamic indicators and/or numerical values in dBm.

- Display the **MAC address** of the wireless cards in the access point. This option may be useful if:
  — You are building the access point name list as described in "AP Names Tab (page 90)"
  — Your network includes RLM's that have been equipped with multiple PC Cards (CP 1515), and you wish to distinguish the cards inserted into the access point specifically

5.2.3.4 Selection Tab

The **Selection** tab enables you to select another network, in situations where you wish to:

- Verify the presence of neighboring networks.
- Determine whether such network might interfere with your network.

Which Access Points RLMs will be displayed when you start the site monitor tool is actually determined by the configuration of the network name parameter on your CP 1515 Manager station (**Edit/Add Configuration Profile** in the **Actions** menu of the main CP 1515 Manager window). For example when the network name of your CP 1515 Manager station is set to:

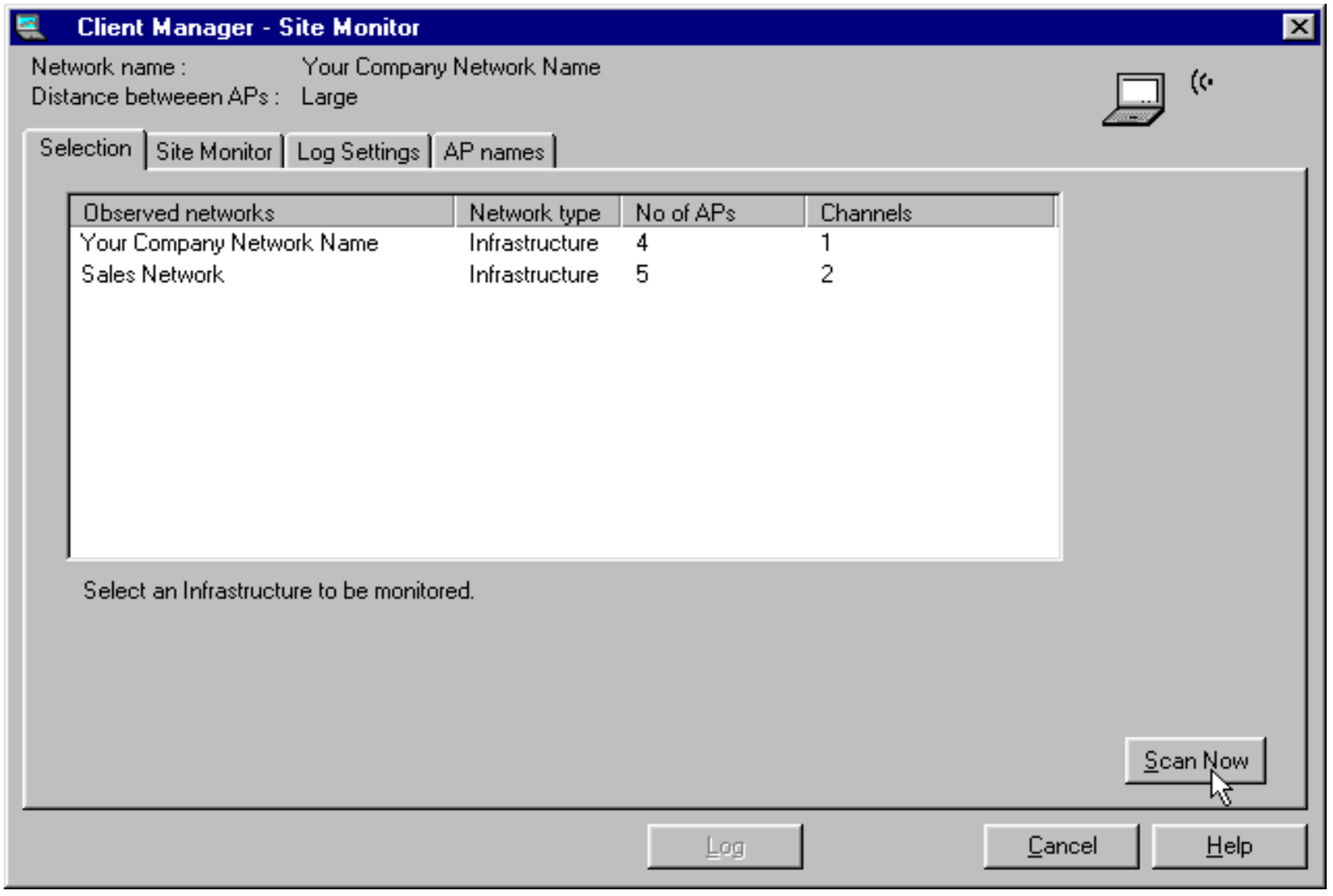
- **A specific Network Name** - the station will:

  - — only connect to an infrastructure network identified by the same network name when the station is powered up.
  - — display only the Access Points RLMs belonging to that network that are within range of your CP 1515 Manager station.
- "**ANY**" network - the monitoring station will:
  - — connect to the first "open" network it sees when the station is powered up.
  - — display all RLMs belonging to that network that are within range of your CP 1515 Manager station.
- **Peer-to-Peer** workgroup:
  - — a workgroup is created between stations with the setting Peer-to-Peer.

5.2.3.5 Selecting another Wireless Network:

1. Click the **Selection** tab on the Site Monitor window to display the window pictured in Figure 16 Select another Network to Monitor.

Figure 16 Select another Network to Monitor



The list of **Observed Networks** on this tab will show:

- All networks that are operational within the range of your CP 1515 Manager station.
- The type of network that might either be an:
  - Infrastructure network
  - Peer-to-Peer workgroup
- The number of Access Points RLMs in the observed infrastructure network(s).

- The different radio channels used by the Access Points RLMs.

2. (Optional) Click the **Scan Now** button to refresh the list of observed networks.
3. Click the network of your choice to return to the Site Monitor tab and display the diagnostic indicators[1].

NOTE:

For reasons of security, the site monitor will not display the network name, and the MAC address or Radio Link Module names of the neighboring network. You can display these values only for the infrastructure network to which you are actually connected.

When the list of **Observed Networks** does not show other networks, this means that:

- Your CP 1515 Manager station has been configured with a specific Network Name.
- This setting will not allow you to scan for/monitor other network infrastructures. To do so, you will need to reconfigure your station to use the Network Name "ANY."
- There are no other networks operational in the vicinity of your CP 1515 Manager station, or

1. Although the Site Monitor Selection tab will allow you to determine the presence of a neighboring Independent (Ad-Hoc) network, you can not select this type of networks for Site Monitor statistics. This is because this feature requires the presence of Access Points RLMs, that are typically not available in Independent networks (see also Wireless Configurations (page 24).

- The neighboring networks have been “closed” to deny wireless compliant devices to establish a radio connection when these devices have been configured with:
    a. The network name “ANY”, or
    b. A zero-string SSID (the equivalent of the network name “ANY”).

  For more information about “open” and “closed” networks, please consult Security (page 154).

5.2.3.6 Log Settings Tab

You can record the Site Monitor measurement results to a log file, and use this log file to more fully analyze the overall wireless coverage of your network. The measurement data can be logged automatically at regular intervals or manually upon user-command.

For more information on log files, see 5.2.4 Logging Measurement Data.

5.2.3.7 AP Names Tab

The **AP names** tab enables you to create a user-defined list of RLM names associated with the MAC address of the wireless network interface(s) of your Access Points RLMs.

The field **AP name** in the Site Monitor window will display the value of the **System Name** parameter that has been assigned to the Access Point RLM upon configuration[1].

1. To assign a system name to the Access Point RLM, you will need the RLM Manager program specify this name in the “SNMP Parameters” window as pictured in Figure 41 Setup SNMP parameters.

To display this name it is required that your computer first establishes true data connections with such Access Points RLMs. This means your computer did not yet:

- Walk around
- Use the **AP Names** tab

When you are running the CP 1515 Manager tool in site monitor mode, you can use the **AP Names** tab to assign the Radio Link Module name “on-the-fly” to any Access Point RLM MAC address that you spot.

When you spot Access Points RLMs identified as “unknown” proceed as follows:

1. Open the tab **AP names**.
2. Enter a MAC address or double-click on one of the MAC addresses in the list.
3. Enter a name that allows for easy identification of this Radio Link Module in the Access Point RLM **Name** field.
4. Next click the **Add to Table** button to associate the name with this MAC address.
5. Repeat steps 2 through 4 for all other MAC addresses.
6. When finished return to the **Site Monitor** tab to proceed with the site monitor survey.

When walking throughout the wireless networking environment, you may see new MAC addresses appear when approaching other Access Points RLMs. If that is the case, repeat the steps described above to complete your Access Point (RLM) **Name** table.

The Radio Link Module names you assign to a spotted MAC address will be saved into an ASCII file that you can use to:

Share the file with other LAN Administrators that use the CP 1515 Manager tool to monitor performance of the wireless network. This file ("APlist.txt") is stored in:

C:\Programs\Siemens I-Gate\Clientmanager

- Edit the names later on, using an ASCII editor, such as the MS-Windows Notepad.

5.2.4 Logging Measurement Data

Both link test and site monitor enable you to log measurement results. The measurement data can be logged manually or at regular intervals automatically.

The CP 1515 Manager saves the data to a Comma Separated Value (*.csv) file that can be imported into standard spreadsheet or database applications for further analysis.

Comparison of measurement data with previous measurements may help you investigate the performance of your wireless LAN over a period of time, for example, to analyze the consequences of relocated network equipment.

Both the Link Test window and the Site Monitor window have almost the same log settings parameters. The only difference is that the Link Test window supports continuous data logging, which the Site Monitor window does not support.

5.2.4.1 Manual Data Logging

The manual data logging function allows you to take a snapshot of the measurement data at specific moment in time, e.g. when you are running site monitor to do a site survey or when you are investigating a particular source of interference.

When you choose the manual mode, you may also wish to enable the **Add comments to log** option to allow you to add comments to your logging information, e.g. a description of the location or event. If you enable this option, a dialog box will appear each time you press the **Log Once** button.

The manual data logging option is typically used on CP 1515 Manager stations roaming the network running site monitor.

5.2.4.2 Automatic Data Logging

The automatic data logging function allows you to log the network performance automatically at preset intervals. This may be useful if you wish to monitor recurring events or variation in values over a long period of time.

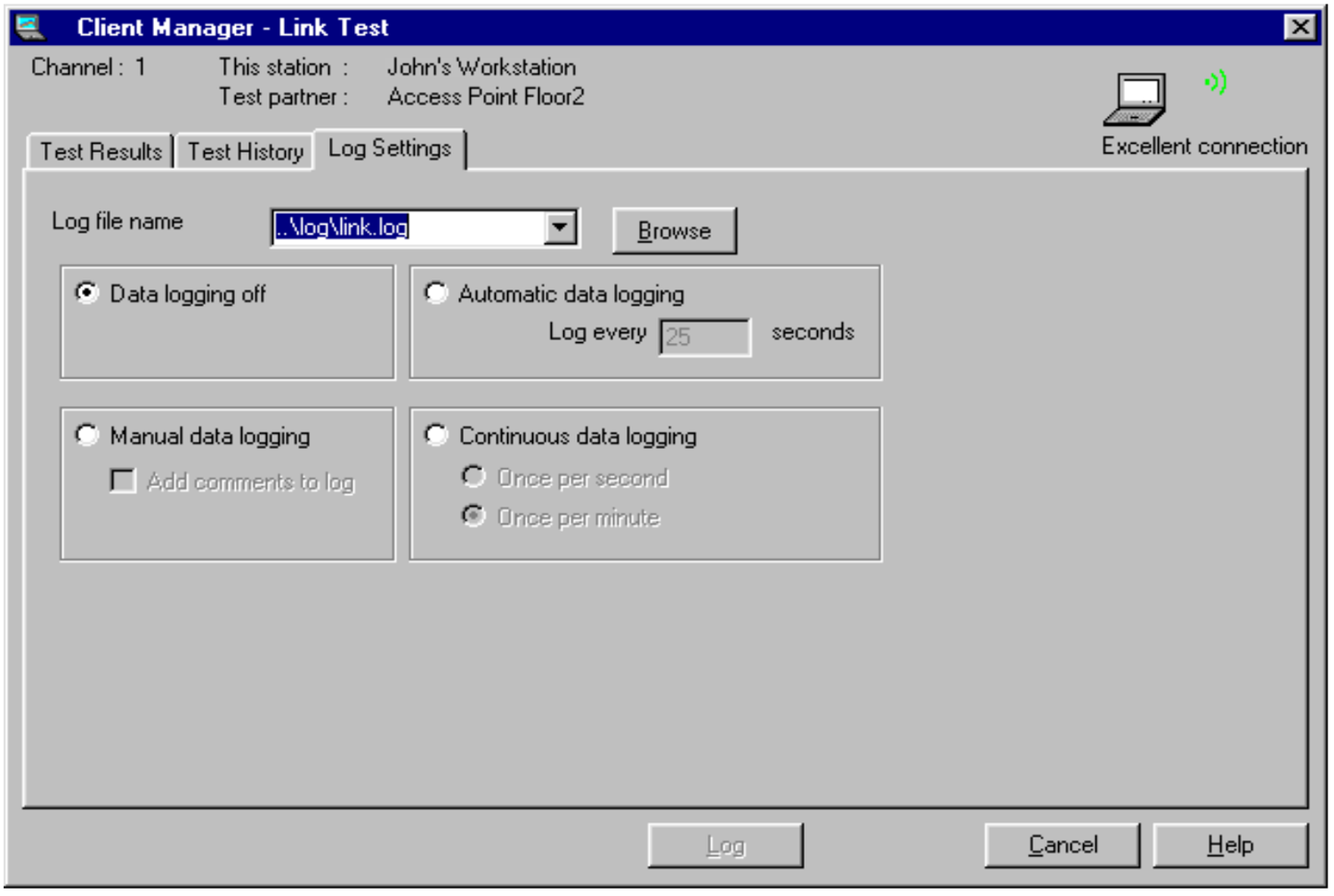
When you choose the automatic mode, you need to set the measurement interval to a specific number of seconds.

Automatic data logging is typically used when the CP 1515 Manager station is running a link test at a particular location.

5.2.4.3 Setting the Logging Options

1. Click the **Log Settings** tab in the Link Test window or in the Site Monitor window to display the window pictured in Figure 17 Log Settings.

Figure 17 Log Settings



2. Enter a filename for your log file in the field **Log Filename**.
   If you:
   - Enter a new filename - a new file is created.
   - Enter the same filename - the data will be appended
   - Use the default filename - the data will be appended.
3. Select the mode of logging:
   - **Data logging off** - no data is logged.

- **Manual data logging** - to manually record your link measurements. Optionally, you can add comments each time you log data by clicking the "Add comments" check box.
- **Automatic data logging** - to automatically log data. You must enter a time interval between measurements.
- **Continuous data logging** (only available in Link Test window) - Automatically log data with the following interval:
  a. **Once per second**, or
  b. **Once per minute**

In all modes, the measurement data is saved in the file entered in the **Log Filename** field. Each time new data is saved, this information is appended to the existing file. If you wish to save the data in a new file, use this field to enter a new filename.

5.2.4.4 Starting/Stopping the Logging Function

Depending on your choice of logging option, the logging button will read either **Log Once** (manual option) or **Start Log** (automatic options).

- For manual logging, click the "Log Once" button each time you wish to log data. Logging stops automatically after the data is recorded to the log file.
- For automatic logging, click the **Start Log** button. Click the **Stop Log** button to stop the logging function.

5.2.5 Diagnose Card

If you suspect that your PC card CP 1515 may not be functioning properly, you can select **Diagnostics** in the **Advanced** menu of the main CP 1515 Manager window to investigate the functionality of the hardware and software of the card.

The Diagnose Card window allows you to check the software and firmware information, configuration information as well as communication statistics.

To test the PC card CP 1515, click the **Test Card Now** button on the **Card Check** tab.

NOTE:

Running the card test will disrupt the normal operation of your PC card CP 1515, which may result in a temporary loss of your connection to the network.

If the PC card CP 1515 passes all tests, the test status will read “OK” in all fields, and the Error Code field will remain blank. If an error occurs, click the **Advice** button for more information on how to handle the error.

5.2.6 Troubleshooting Site Monitor

When the Site Monitor does not display (all of) the Access Points RLMs that you expected, this may be due to one or more of the following reasons:

- Your CP 1515 Manager station is “out-of-range” of the Access Points RLMs that you wish to monitor. Typically the values for signal level and SNR are ‘0’ (zero).
- A configuration mismatch of your CP 1515 Manager station, for example:
  - Your CP 1515 Manager station uses a specific network name that does not match the name of the infrastructure that you wish to monitor.
  - Your CP 1515 Manager station uses the network name “ANY,” and when it was powered up, the station erroneously connected to the RLM of a neighboring network because that RLM provided the best level of SNR.
- The infrastructure that you wish to monitor has been “Closed” to wireless IEEE 802.11 compliant devices that try to establish a radio connection using:
  - The network name “ANY,” or
  - A zero-string SSID (the equivalent of the network name “ANY”).

When your CP 1515 Manager station uses the network name “ANY,” you can use the **Selection** tab to see other networks as described on Selection Tab (page 86).

For more information on “open” and “closed” infrastructure networks, please consult Security (page 154).

5.3 Using the RLM Manager

You can use the RLM Manager to:

- Display a standard set of SNMP variables to monitor general LAN traffic performance in your network (see Remote Statistics Tab (page 108)).
- Display remote link test measurements (see Remote Link Test Window (page 103)) between a (remote) Access Point RLM of your choice and a wireless station connected to the selected Access Point RLM.

The RLM Manager has been designed to monitor your network from a central location (e.g. the LAN administrator station) enabling you to monitor wireless performance in areas that can not easily be reached. For example: wireless networks in remote locations.

5.3.1 Monitoring Options

The RLM Manager program offers a variety of diagnostic options of which the following two are the most relevant for standard users:

- System information (see System Information (page 101))
- Remote link test (see Remote Link Test Window (page 103))
- Remote statistics (see Remote Statistics Tab (page 108))

All other diagnostic options are standard SNMP tallies that are not described in this manual, but documented in the on-line help system of your RLM Manager program.

NOTE:

All diagnostic options are described in the on-line help information of the RLM Manager. To access that you can access by pressing the F1 function key or clicking the **Help** button in your RLM Manager window.

5.3.2 Connecting to Access Points RLMs

To start monitoring the Radio Link Module, you must first connect to the target Radio Link Module.

1. Start the RLM Manager program.
2. Select the target RLM from the local list or enter the IP address of the Access Point RLM that you wish to monitor.

   Alternatively, you can select **Refresh** Radio Link Module **List** from the RLM menu to display all Access Points RLMs available in your subnet.

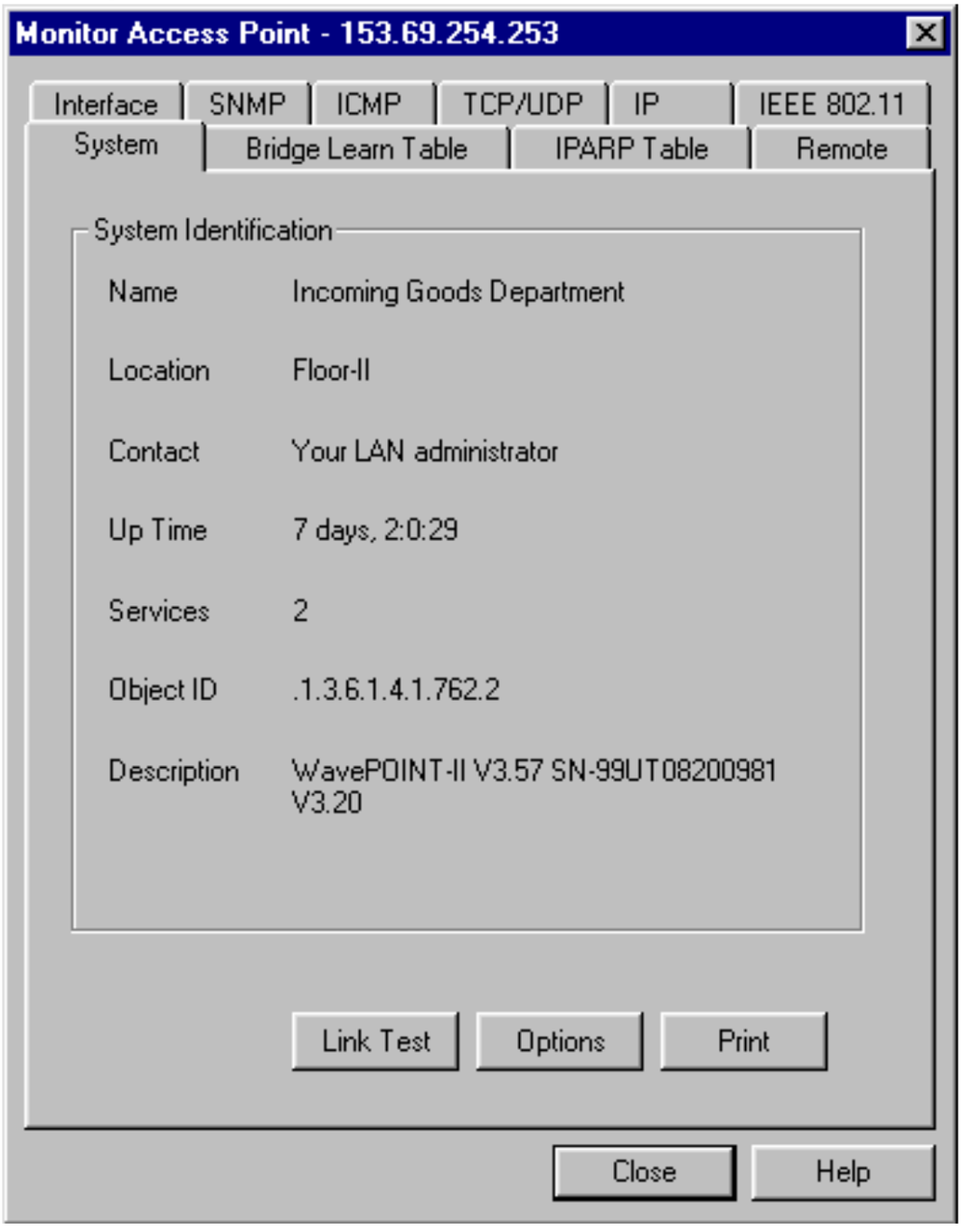
NOTE:

Only Access Points RLMs in the same subnet as the management station are displayed in the list. To investigate a link outside of the subnet, enter the specific IP address in the **Enter the IP address of a specific** Access Point RLM field.

3. Click **Monitor** to connect to the target Radio Link Module.
4. The monitor mode of the RLM Manager window is displayed as pictured in Figure 18 System Information Window.

You can now monitor your network.

Figure 18 System Information Window



5.3.3 System Information

The system information does not provide on-line statistics, but is primarily used to verify the version level of the embedded software that is loaded into the Access Point RLM.

To display the system information for the RLM, you must first connect to the target RLM (see Connecting to Access Points RLMs (page 99)).

Select the **System** tab to view the system information.

- The fields **Name**, **Location** and **Contact** represent the values that have been entered in the corresponding fields of the **SNMP** tab in the edit mode when the Access Point RLM was configured.

  If you would like to change these names, please consult the section about configuring SNMP parameters as described in SNMP Parameters (page 211).
- The **Up Time** field displays the time interval measured from the last time the Radio Link Module was reset. If the up time is lower than expected, the RLM may have been reset manually or rebooted automatically.
- The fields **Services** and **Object ID** do not display relevant information to end-users. You will need these values and the contents of the **Description** field only when contacting Technical Support to report a problem.

  Providing this information to your Technical Support representative will help to determine the cause of the problem.

  To do so, you can either:

- Use the **Print** button to print the information to paper that you will fax to your Technical Support together, or
- Press the keys ALT and Print Scrn simultaneously to copy the contents of this screen to the Windows clipboard, and paste the screen capture into the e-mail that you will send to your Technical Support.

- The field **Description** is the most important field of this screen. It allows you to quickly determine whether the Access Point RLM is running with the latest embedded software, or might require an upgrade to support all the SIMATIC NET IWL functionalities required.

  The **Description** field contains a set of strings to identify:
  - The type of networking device
  - The type and version of the embedded software that is loaded into this Access Point RLM. The value can be:
    - **VX.xx** to identify software that supports access point services only
  - The character string of the format **SN-xxUTxxxxxxxx** represents the unique serial number of the RLM.
  - The last string of characters of the format **VX.xx** identify the version of the RLM hardware in its "processor module."

NOTE:

Updates for the embedded software of the Access Points RLMs are usually released via the MOBIC web site **http://www.siemens.com/mobic**, and with new releases on the software CDs.

You are advised to consult the MOBIC web site at regular intervals to find out whether newer software is available for your Access Points RLMs.

5.3.4 Remote Link Test Window

The RLM Manager remote link test enables you to investigate the radio link between the Access Point RLM of your choice (the "initiator station") and a station connected to the selected RLM.

This station can be a wireless station connected to the selected RLM.

NOTE:

The remote link test works only in combination with SIMATIC NET Radio Link Modules RLM.

The user-interface of the RLM Manager Remote Link Test is very similar to the Link Test of the CP 1515 Manager.

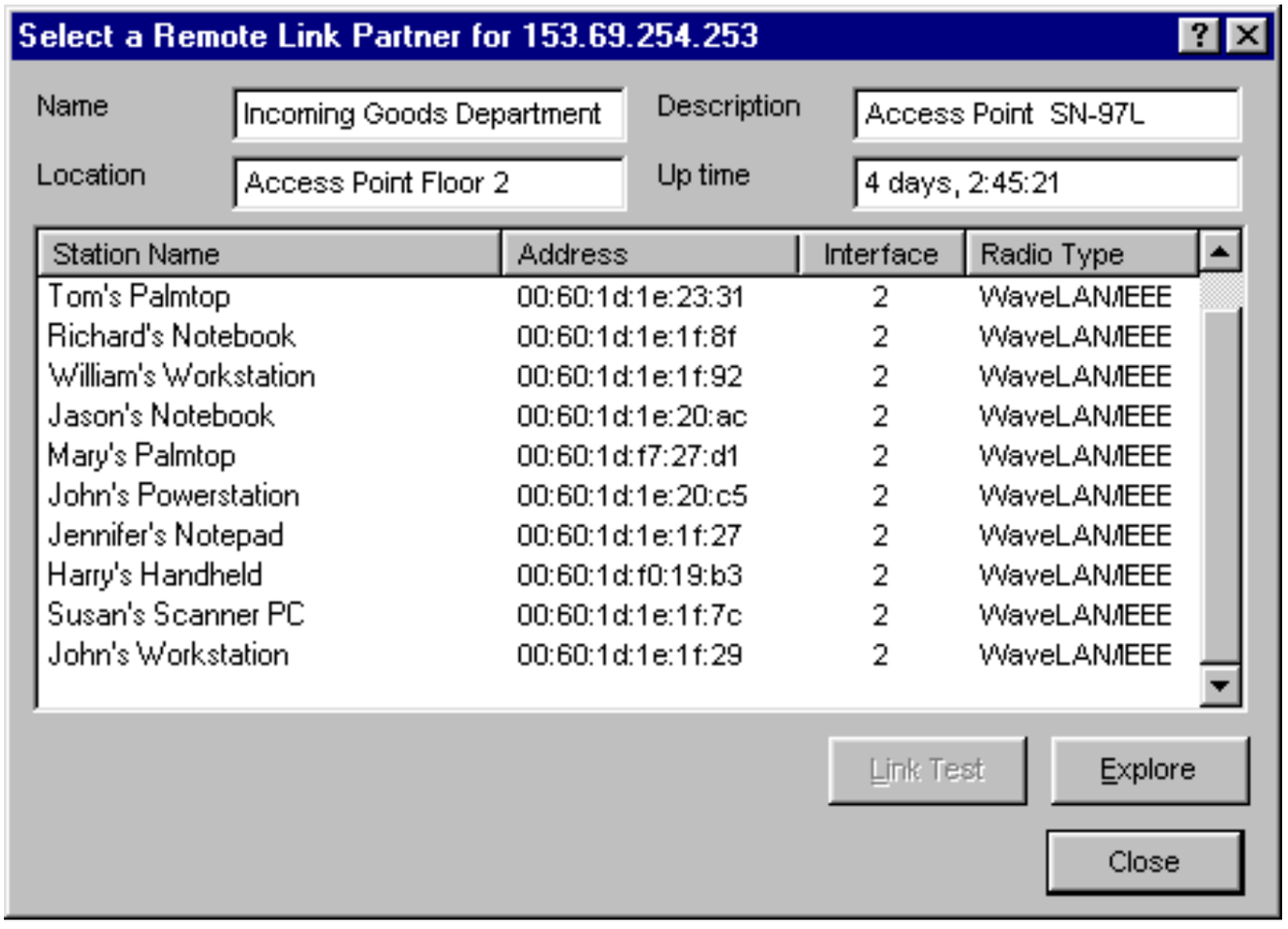
5.3.4.1 Starting the Remote Link Test

To display the remote statistics for the Radio Link Module, you must first connect to the target RLM as described in Connecting to Access Points RLMs (page 99).

1. Select the **System** tab and click the **Link Test** button to display the window pictured in Figure 19 Select a Link Test Partner.

   The fields in the top section of this window identify the "initiator station" you selected when connecting to the Access Point RLM.

Figure 19 Select a Link Test Partner



The middle section of the "Select Remote Link Partner for ..." window displays all wireless devices connected to the "initiator station." The following fields are visible:

- The fields **Station Name** and **Address** these wireless devices are identified by their station name and MAC address respectively.

  This list may change as roaming mobile stations enter or exit the coverage area of the selected RLM.
- The **Interface** field identifies the slots of the Radio Link Module into which the PC Card CP 1515 has been inserted.

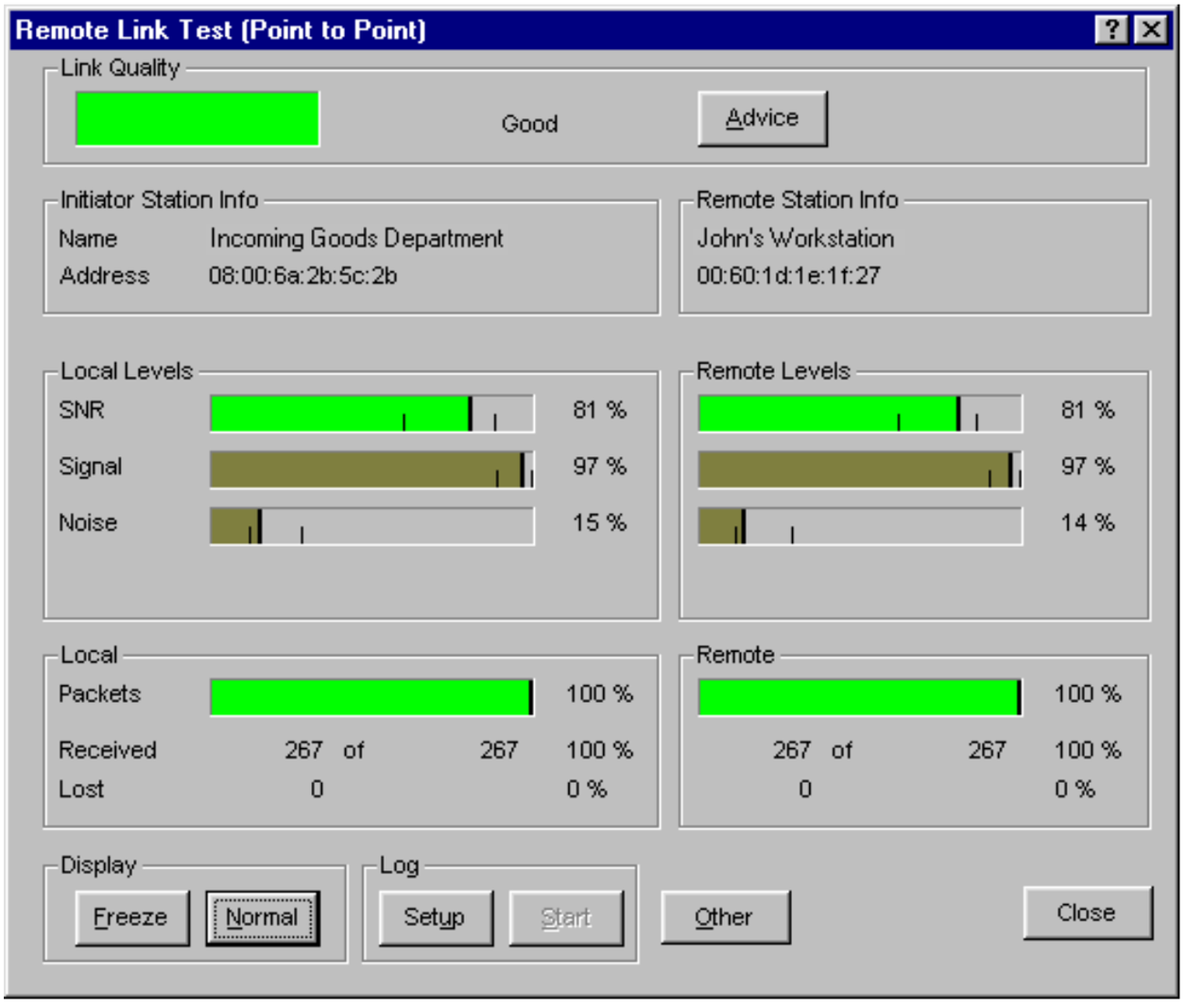
  - — 2 = PC Card slot A
  - — 3 = PC Card slot B
- The **Radio Type** field identifies the type of PC Card (in the corresponding slots):
  - — IEEE 802.11 for PC Cards (CP 1515)

2. (Optional) To refresh the list, click the **Refresh** button.
3. Select a station from the list and click the **Link Test** button to display the Remote Link Test window as pictured in Figure 20 Remote Link Test window.

NOTE:

Subject to the "Radio Type" of the wireless network interface that you selected, the lay-out of the Remote Link Test windows may differ. The window pictured in Figure 20 Remote Link Test window represents the window for the wireless network interface.

Figure 20 Remote Link Test window



5.3.4.2 Important Indicators to Monitor

The Signal to Noise Ratio (SNR) identifies the communication quality of the radio path between the initiator station and its remote link test partner.

The color of the SNR indicator, the link quality indicator, and the remote levels indicators relate to the following levels of communications quality:

Color	Description
• Green	Communication quality is "Good," no intervention is required.
• Yellow	Communication quality is "Marginal," no intervention is required.
• Red	Communication quality is "Poor," intervention required. (see Troubleshooting (page 236))
• Blank	No connection

If the level of SNR is lower than expected the signal and noise level indicators may help you investigate the cause.

Click the **Details** button to show the signal and noise level indicators.

- A low signal level indicates that the "strength" of the radio signal is fairly low, i.e. the Access Point RLM selected link test partner has moved "out-of-range."
- A high noise level indicates a source of radio interference in the radio path between the RLM and its link test partners.

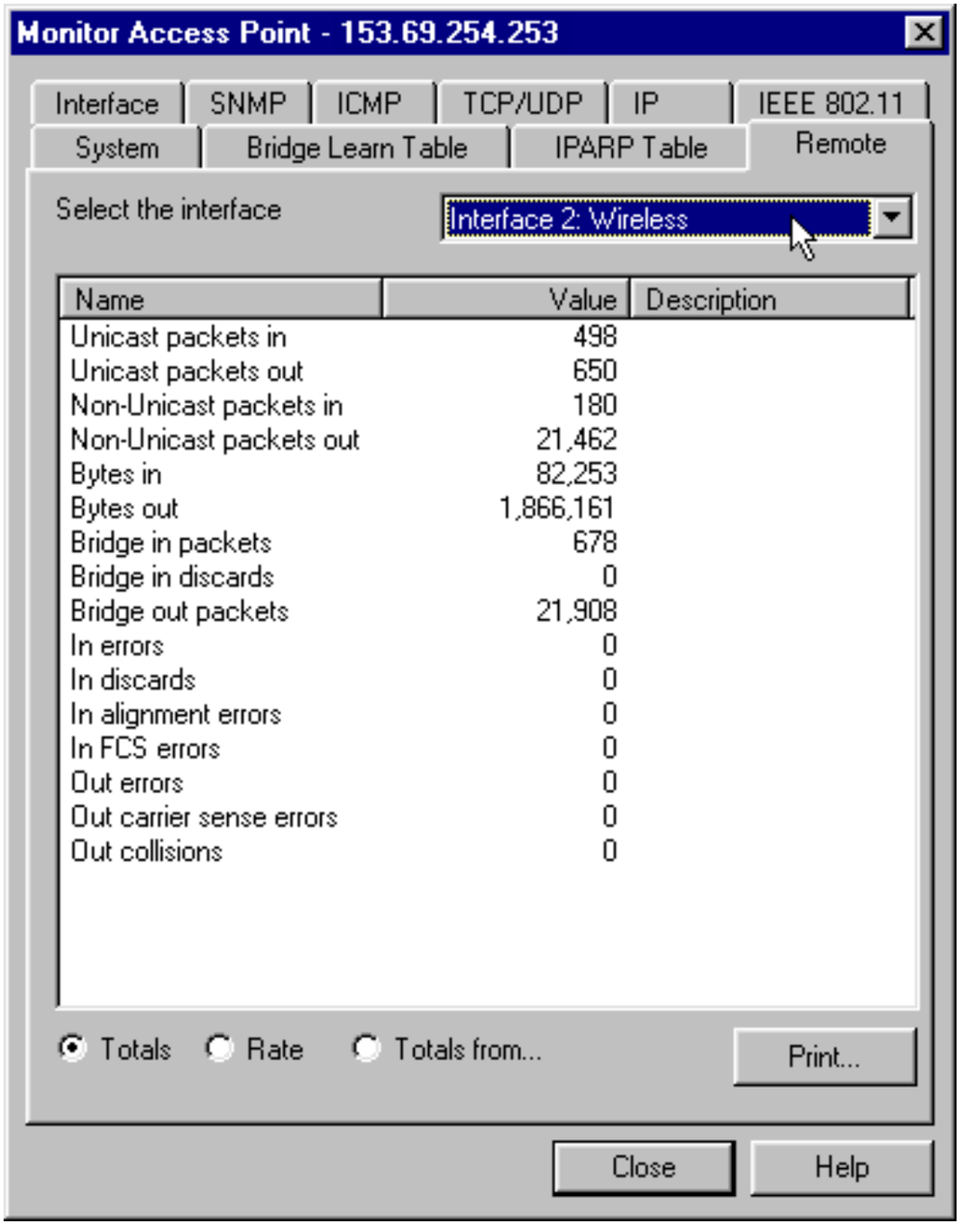
Comparing the values for the Access Point RLM and its link test partner will help you to identify the location where the interference occurs, and investigate whether any actions to eliminate or remedy the source interference resulted in a better performance.

For more information about the Remote Link Test window please consult the RLM Manager on-line help documentation by clicking the **Help** button or pressing the F1 function key on your keyboard.

5.3.5 Remote Statistics Tab

The remote statistics option allows you to monitor a set of SNMP variables for each of the RLM interfaces (both Ethernet and wireless).

Figure 21 Remote Statistics information



5.3.5.1 Starting Remote Statistics

To display remote statistics for the Radio Link Module, you must first connect to the target RLM as described in Connecting to Access Points RLMs (page 99).

1. To view the remote statistics, select the **Remote** tab from the RLM Manager window in the monitor mode (see Figure 21 Remote Statistics information).

The performance for each of the interfaces of the selected Access Point RLM can be displayed. Selecting the interface of your choice from the **Select the interface** pull down menu.

5.3.5.2 Important Indicators to Monitor

The RLM Manager **Remote** tab statistics display a wide range of variables that provide information about the performance of the selected RLM.

The indicators which provide the main monitoring information is called the **ratio of Errors to Bridge Packets**. There are three ratios which are of particular diagnostic value:

- In errors / Bridge in packets
- Out errors / Bridge out packets
- Out collisions / Bridge out packets

The following table provides diagnostic information relating to each of these three ratios.

Table 1 Ratio of Errors to Bridge Packets.

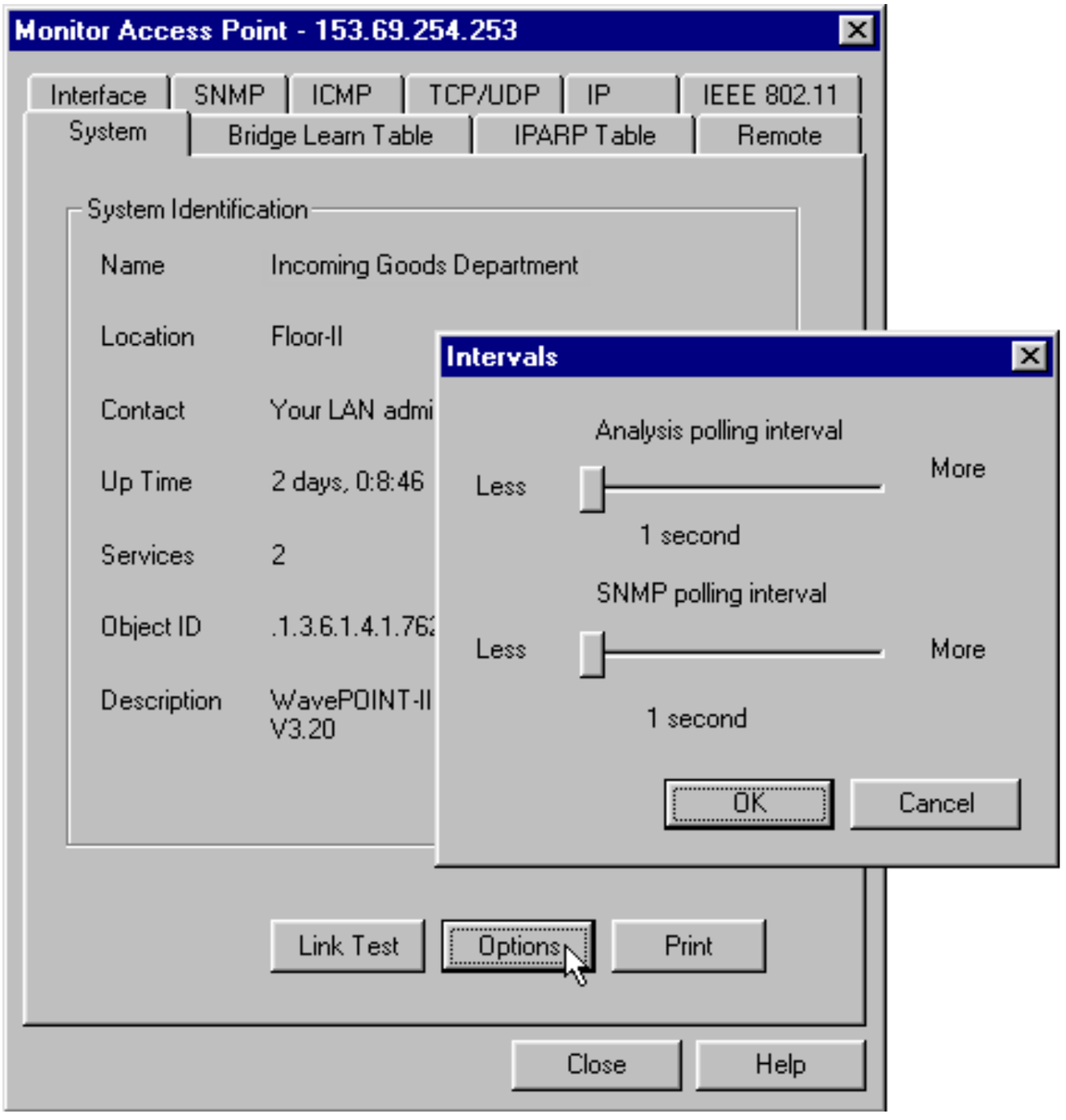
Ratio Errors to Bridge Packets	Conclusion	
0.1% or less	Status:	Performance is Good.
	Impact:	None.
	Action:	None.
0.1% and 1%	Status:	Performance is acceptable.
	Impact:	Network performance is OK, but your network might not do as well as you expected.
	Action:	Refer to Optimizing Performance (page 116) to determine the cause of the problem and optimize your network performance.
1% or more	Status:	Performance is poor.
	Impact:	The performance problem may be caused by your network cabling or connections.
	Action:	Refer to Optimizing Performance (page 116) to solve the problem.
2% or more	Status:	Performance is very poor.
	Impact:	Your network operating system is likely to face severe performance problems.
	Action:	Refer to Optimizing Performance (page 116) to investigate the problem in more detail. You may need to consult an external expert.

5.3.6 System Intervals

To display the system interval parameters to monitor the RLM, you must first connect to the target Access Point RLM as described in Connecting to Access Points RLMs (page 99).

Select the **System** tab and click the **Options** button to display the window pictured in Figure 22 Intervals window.

Figure 22 Intervals window



In the Intervals window two different time interval parameters can be set to change to monitor interval settings:

- Analysis polling interval (used for remote link test)
- SNMP polling interval (used for SNMP statistics).

5.3.6.1 Adjusting Analysis Polling Interval

Subject to the type of connection, you can adjust the refresh rate of the remote link test results, also identified as the analysis polling interval.

While the remote link test will proceed to continuously collect measurement results, the selected Radio Link Module (initiator station) will transfer the results to the LAN administrator station at regular intervals, which can vary from 1 to 15 seconds.

- Use a short time interval (e.g.1 second) for on-line monitoring, e.g., when troubleshooting or when you have full bandwidth access via the local network.
- Use a longer time interval (e.g. 15 seconds) when you run a remote link test only for background information purposes, or in cases when you access the initiator stations network via a low-speed connection (e.g. a dial-up modem connection).

5.3.6.2 Adjusting SNMP Polling Interval

The data displayed in the **Remote** tab refreshes at regular intervals that can vary between 1 second and 5 minutes. Adjust the refresh rate by changing the SNMP polling interval.

- Use a short interval (1 second) when you want to monitor remote statistics on-line, e.g. in case of troubleshooting and/or when you have full bandwidth access to the RLM via the local network.
- Use a long interval (5 minutes) when you run remote statistics only for background display purposes, in cases when you access the network of the selected Radio Link Module via a low-speed connection (for example a dial-up modem connection).

6 Optimizing Performance

6.1 Introduction

The performance of your LAN is usually determined by a complex combination of different factors. This section will present a number of considerations that may help you to:

- Determine whether optimization is really needed,
- Tailor your SIMATIC NET IWL network to optimize its performance.

Consider optimizing network performance in these situations:

- You are troubleshooting a suspected problem
- LAN performance is less then expected, or
- Routine checks at regular intervals show a performance degradation.

In this chapter, we recommend various solutions to some of the most commonly reported problems.

CAUTION:
Create separate backup files of the configuration data for each Access Point RLM, before you start changing the configuration(s). Doing so will enable you to restore the initial setup of your network in case corrective actions did not result in the desired effect.

6.2 Eliminating Redundant Traffic

Data transmitted via your network can be divided in two major types of data:

- True Data - is data communicated between network stations, such as file-transfer or e-mail. This "True Data," usually referred to as "payload," also includes messages that were retransmitted one or multiple times as a result of a collision, malfunctioning cable connection or poor radio link.

  In the RLM Manager Remote tab in the monitoring mode, the "True Data" is displayed as Unicast Packets.
- Network Overhead Data - is data exchanged between network services to control the dataflow. This overhead data that usually referred to as "traffic load," includes protocol and broadcast messages and/or error messages that result from a configuration mismatch.

  In the RLM Manager Remote tab in the monitoring mode, the "Network Overhead Data" is displayed as Non-Unicast Packets.

The ratio of network overhead in relation to "True Data" differs from one networking service to another. However when the ratio of network overhead is more than actually required, this may affect the performance of your wireless LAN, because your "True Data" has to share the bandwidth capacity with the network overhead.

Eliminating redundant traffic can significantly improve the performance of your network. Using the RLM Manager you can choose from one or more of the following options:

- Protocol Filtering (page 118): to filter protocols that are not relevant to wireless stations.

- Optimizing Wired Connections (page 121): to eliminate redundant error messages due to failing connections.
- Optimizing Wireless Connections (page 125): to avoid retransmission of lost or collided frames.

6.2.1 Protocol Filtering

Some network protocols send large volumes of broadcasts to all stations. In many cases, these protocols may not be required by your wireless stations. In these cases, protocol filtering may prevent the transmission of unnecessary data, saving more bandwidth for the communication of "true data" in your network.

6.2.2 Do You Need Protocol Filtering?

To diagnose whether or not the protocol broadcasts degrade the performance of a wireless network, you can use the Remote Statistics tab as described on Remote Statistics Tab (page 108).

1. Start the RLM Manager and select the Access Point RLM and click the **Monitor** button.
2. From the **Monitor** menu, select **Remote Statistics**.
3. Select the **Remote** tab to display the interface statistics.
4. Compare the number of **Out collisions** with the number of **Bridge out packets**.

- When the number of "Out collisions" is less than 1% of the "Bridge out packets," this indicates that the wireless medium is performing fine, i.e. protocol filtering is not required, but might still be considered.
- When the number of "Out collisions" is more than 1% of the "Bridge out packets," this indicates that the wireless medium is very busy.

  If the wireless medium is busy, and you do not see many users or excessive traffic on the network, it might be worth investigating whether protocol filtering will improve your network performance.

5. Compare the number of **Unicast packets out** to the number of **Non-Unicast packets out**.
   - When the number of "Non-Unicast packets out" is relatively high when compared to the number of "Unicast packets out," this might indicate your network generates a large amount of network traffic.

     This does not necessarily mean that the traffic load is caused by the protocols, but it might be worth investigating whether protocol filtering will improve your network performance.

CAUTION:

It may require advanced networking expertise to identify which protocols are used within your network, and to decide which protocols can be filtered without affecting the proper operation of your network operating system.

6.2.3 Filtering Network Protocols

When you suspect that network protocols are adversely affecting the performance of your network, use the following procedure to filter out unnecessary or unwanted network protocols.

1. Investigate what type of network stations and services are located in the environment of your network.
2. Consult the documentation that came with your network operating system to investigate which protocols are required for network servers and services, and for the (wireless) stations.
3. Start the RLM Manager program.
4. Select the Radio Link Module of your choice and click the **Edit** button.
5. Select the **Bridge** tab to show the protocol filtering information.
6. On the top-right side of the protocol filtering section, click the **Edit** button to open the Protocols to Filter window (pictured in Figure 37 Select Ethernet Protocols to be Filtered).
7. Place a check mark for all protocols that you wish to filter.
8. (Optional) To add a non-listed protocol to the list, click the **Custom** button to enter the protocol manually.
9. When finished click **OK** to return to the **Bridge** tab.

   All of the protocols that you have selected, and/or all of the custom protocols that you have added manually, will be listed in the **Protocol Filtering** field.
10. Click **OK** again to save the changes to the Access Point RLM and to return to the main window of the RLM Manager.

11. Download a backup file as described in Step 4 - Create a Back-up of the Configuration (page 66).

    When prompted to enter a name for the back-up file, you are advised to select a name that is different from the original configuration file.
    Do not overwrite the previous version of the back-up file, since this might jeopardize your ability to restore the original configuration if this change did not result in the expected performance increase.

Repeat the steps as described under Do You Need Protocol Filtering? (page 118) to see whether this change resolved your problem. If this does not solve your problem, consider one of the following options:

- Optimizing wired connections
- Optimizing wireless connections

6.2.4 Optimizing Wired Connections

Sometimes performance degradation of your (wireless) connection is caused by a failure in the cabling system that connects the network to the wired infrastructure.

Such failures may be caused by one of the following situations:

- A faulty cable or connector in the wired infrastructure
- A LAN segment that has been stretched over a distance that is too long.

Usually what will happen in this kind of situation is that:

- The system does not work at all, or

- Your network system will generate a large number of error messages as a result of the faulty connection(s). As these messages are taking up bandwidth, the performance of your network may become very slow.

6.2.5 Checking the Cable System

The occurrence of a problem in the cabling system can be diagnosed with the remote statistics found on "Remote" tab in the monitor mode of the RLM Manager.

1. Select **Interface 1: Ethernet** from the pull-down menu to display the statistics for the Ethernet interface.
2. Compare the number of **In errors** with the number of **Bridge in packets**.
   - When the number of "In errors" is 1% or more of the "Bridge in packets", this may indicate a cabling problem.
3. Compare the number of packets **Out errors** with the number of **Bridge out packets**.
   - When the number of "Out errors" is 1% or more of the "Bridge out packets", it is likely that there is a cabling problem.
4. Compare the number of **Out carrier sense errors** with the number of **Bridge out packets**.
   - When the number of "Out carrier sense errors" is 1% of the "Bridge out packets" or the value of the "Out carrier sense errors" increases too rapidly, this indicates insufficient space on the network due to a backbone overload, or faulty cabling.

5. Check whether the problem occurs only with the selected RLM, or with multiple Access Points RLMs.
   - If the problem is observed on only one Access Point RLM, the problem may lie in the connectors or cable(s) that connect the Radio Link Module to the hub or wired backbone.
   - When the problem exists with multiple Access Points RLMs, it is likely to be caused by the cables or connectors of the wired backbone, hub or the bridge/router device that connects this network segment to your LAN.

6.2.5.1 Troubleshooting Cabling Problems

Using the procedure described above, you may have determined the area where a cabling error might be suspected. To resolve the problem, carefully check the cabling system in this area to verify whether all connectors are properly seated at the:

- Access Points RLMs
- Bridges, routers and hubs
- Wired stations connected to the cabling system.

If your network uses BNC coax cable (10Base2), make sure that terminators are placed on both ends.

6.2.6 Checking the Length of Your LAN Segments

In exceptional cases, networking problems may be caused by LAN segments that have been stretched over (too) large distances.

In these situations, frequent collisions might occur because stations can no longer detect the carriers transmitted by distant stations. Collided frames will no longer be received by the addressed station.

The occurrence of a LAN segment system that is too long can be diagnosed with the remote statistics found on the **Remote** tab in the monitor mode of the RLM Manager.

1. Select **Interface 1: Ethernet** from the pull-down menu to display the statistics for the Ethernet interface.
2. Compare the number of **In errors** with the number of **Bridge in packets**.
   - When the number of **In errors** is 1% of the **Bridge in packets** or more, there may be a cabling problem.
3. Monitor the value increase of the parameter **Bytes in** over a longer period of time.
   - When this number increases constantly with more than 600,000 bytes per second, this may indicate a problem with the length of your LAN segment.

You may need to consult a network expert to verify and/or adjust the length of your cable segments.

NOTE:

If you decide to split the LAN (segment) into multiple (sub) segments, make sure that all SIMATIC NET Industrial Wireless LAN equipped devices will be grouped into the same LAN segment. Wireless stations will not be able to roam between LAN segments that are separated by routers and/or gateways.

If this does not solve your problem, consider one of the following options as described in this chapter:

- Protocol Filtering (page 118)
- Optimizing Wireless Connections (page 125)

6.2.7 Optimizing Wireless Connections

When the link quality of communications between a wireless station and its Access Point RLM is poor, packets communicated between this station and the Radio Link Module may get lost. Waiting in vain for an acknowledgment of the receiving station, the sending station will re-transmit the lost packet.

Upon receipt of the same packet for the second time, the receiving station might decide to discard all packets received so-far, which would require that the sending station will have to retransmit all packets once again.

Please note that:

- Many retransmissions may affect your effective data throughput efficiency as the “true data” has to share the wireless bandwidth with the re-transmitted frames.

- The retransmissions will also degrade the performance as perceived by the end-user of a wireless stations: e.g. saving a file will take longer if many retransmissions are required.

A poor link quality can be caused by one or more of the following problems:

- The station is almost out of range of the Access Point RLM.
- There is a source of interference in the signal path between the station and the Radio Link Module.
- A station may be “hidden” from another station within the same coverage area (for more information on hidden stations, see the section RTS/CTS Medium Reservation (page 131)).

6.2.8 Diagnosing Link Quality

The occurrence of a poor link quality on the wireless network can be diagnosed in different ways.

- You can use the RLM Manager tool to diagnose the quality of radio communications on-site as described in Monitoring your SIMATIC NET IWL Network (page 67), or
- Use the RLM Manager tool to investigate from your current location whether a specific remote area is suffering from poor radio performance.

  The RLM Manager provides the following options to diagnose radio link quality:

  — The remote link test
  — The IEEE information
  — The Remote Statistics tab

These tallies can be useful in determining whether or not the performance of your network is caused by interference.

6.2.8.1 Remote Link Test

For instructions about the Remote Link Test window that displays communications as dynamic indicators, please refer to the information about this window as described on Remote Link Test Window (page 103).

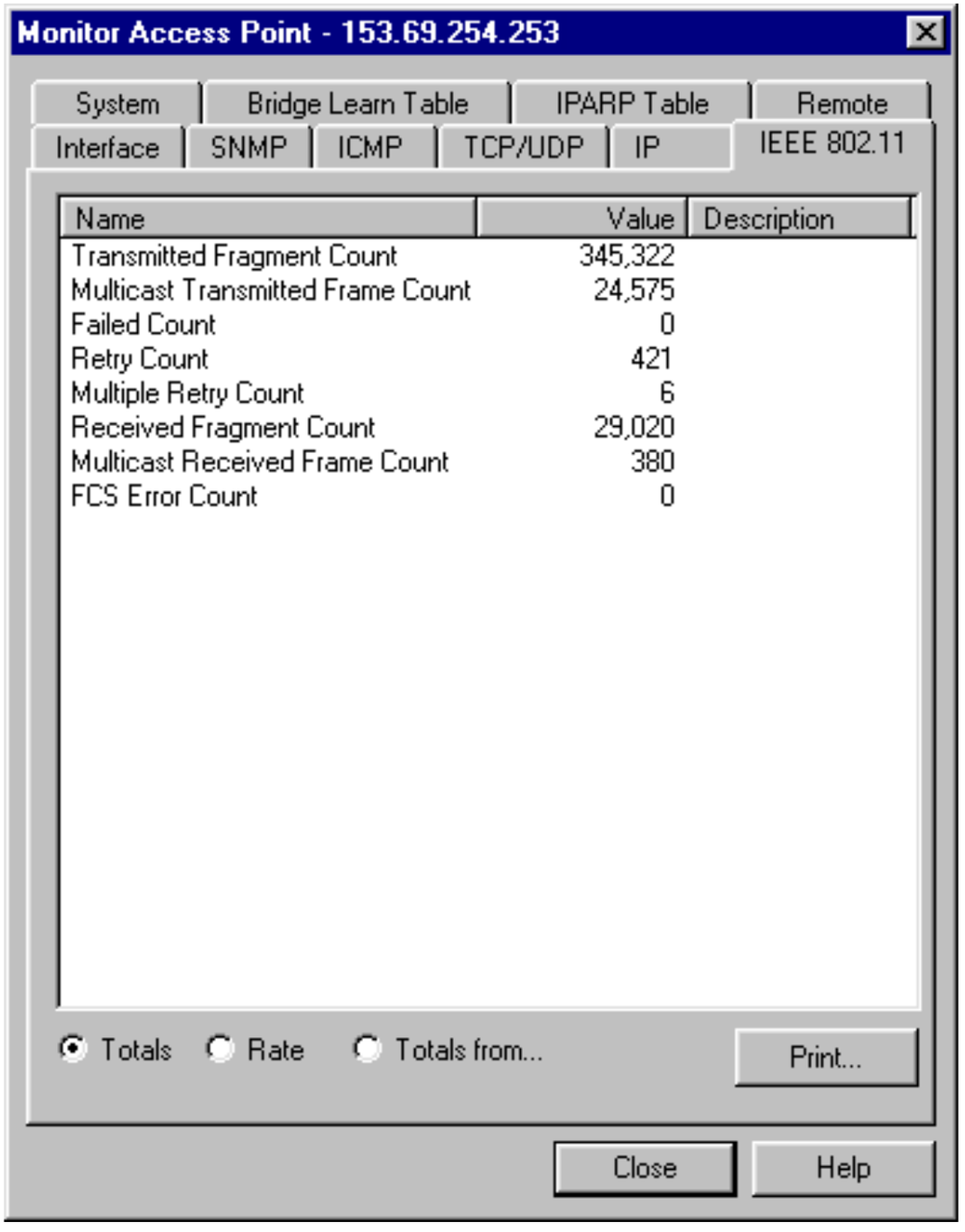
Important indicators to monitor on the Remote Link Test window are:

- Signal to noise ratio (SNR) for an overview of the radio link quality.
- Signal level to determine whether a poor SNR is related to a weak radio signal (i.e. a station is “out-of-range”).
- Noise level to determine whether a poor SNR is related to a source of interference.

6.2.8.2 IEEE Information

The IEEE information on the **IEEE 802.11** tab in the monitor mode allows you to track frame activity on the IEEE interface of the Access Point RLM.

Figure 23 IEEE information tab



The three indicators that you should pay particular attention to are:

- **Retry Count** - counts the number of frames that are lost (due to collisions) during the initial transmission. During normal operation, the **Retry Count** should be less than 3% of the **Transmitted Fragment Count**.
- **Multiple Retry Count** - counts the number of frames that are lost after the initial transmission. During normal operation, the **Multiple Retry Count** will be less than 3% of the **Retry Count**.
- **Failed Count** - counts the number of frames that have reached the **Retry Limit**. Failed frames will no longer attempt to re-transmit.

  If the **Failed Count** is 1% or more of the **Multiple Retry Count**, your network may be suffering from interference. Use the RLM Manager Remote Link Test Window (page 103) to look for either suddenly high noise figures, or low SNR values, to find the cause of the interference.

6.2.8.3 Remote Statistics Tallies

Select the **Remote** tab in the monitor mode. Select either one of the interfaces from the pull-down menu to display the statistics for the wireless network interface(s). Then, use the following to diagnose link quality:

1. Compare the number of **In errors** with the number of **Bridge in packets**.
   - When the number of "In errors" is 1% or more of the "Bridge in packets," this may indicate that the wireless medium is very busy.
2. To verify this assumption, also compare the number of packets "Out errors" with the number of "Bridge out packets."

- When the number of **Out errors** is 1% or more of the **Bridge out packets**, it is likely that one or more stations suffer form a poor link quality.

3. Compare the number of packets **Out collisions** with the number of **Bridge out packets**.
   - If the number of **Out collisions** is 1% or more of the **Bridge out packets**, it is likely that the wireless medium is very busy. This might be caused by many retransmitted frames, but it could also refer to many stations trying to communicate at the same time.
4. You can also use the RLM Manager remote link test to analyze whether one or more stations show a poor link quality:
   - When the poor link quality is caused by a low signal level, the station is almost out of range of the Access Point RLM.
   - When the poor link quality is caused by a high noise level, there is a source of interference in the signal path between the station and the Radio Link Module.
5. When one or more stations show a poor link quality, re-transmissions of frames will disturb overall statistics and performance.
   - You may be able to solve the problem by either moving the station(s) or eliminating the source of interference.
   - If the problem is a poor signal you may consider:
   — Connecting a range extending antenna to the station or access point that suffers from poor radio performance.
   — Adding an extra Access Point RLM to the network, or
   — Adjusting the placement of your Access Points RLMs to provide coverage for all wireless stations.

- If you suspect a “hidden” station, see RTS/CTS Medium Reservation (page 131).

NOTE:

You can also use the CP 1515 Manager to analyze the link quality between a remote station and the Access Point RLM. In that case, you will need to have access to the “problem location” to do on-site diagnostics.

If these options do not resolve your problem, consider one of the following options:

- Protocol Filtering (page 118)
- Optimizing Wired Connections (page 121)
- Designing High Capacity Networks (page 146)

6.2.8.4 RTS/CTS Medium Reservation

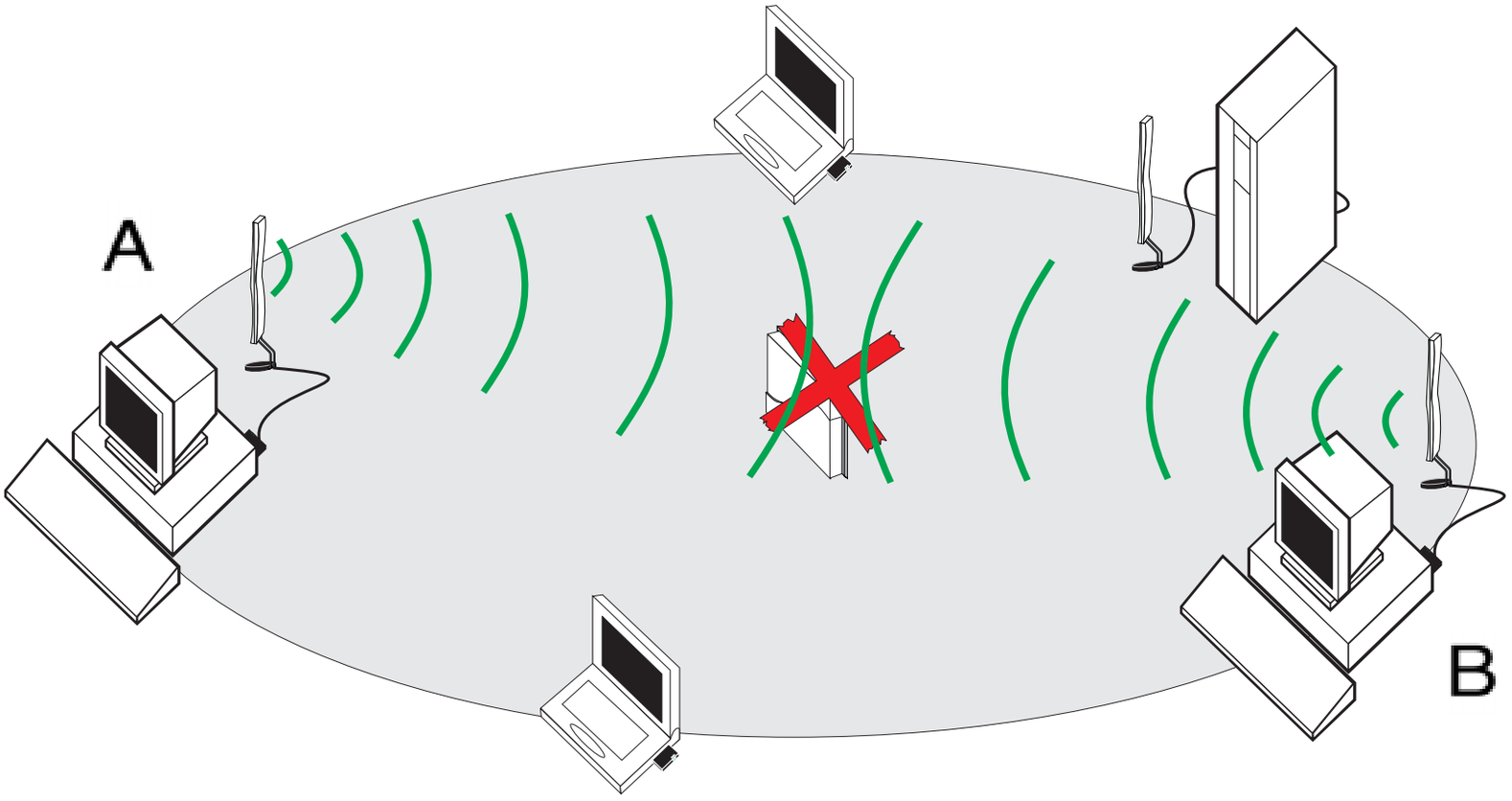
It is normal behavior for SIMATIC NET IWL stations to defer transmissions automatically when they sense that another wireless device is using the wireless medium.

This behavior also referred to as the Carrier Sense Multiple Access/Collision Avoidance protocol (CSMA/CA) will avoid that wireless messages would collide in situations where two or more stations would start transmissions at the same time.

The RTS/CTS medium reservation mechanism enables you to improve wireless performance in network environments where the CSMA/CA

protocol would fail due to the “hidden station” problem as pictured in Figure 24 The Hidden Station Problem.

Figure 24 The Hidden Station Problem



RTS/CTS medium reservation may provide a solution for networks where:

- The density of stations and Access Points RLMs is very low.
- You witness poor network performance due to excessive frame collisions at the Access Points RLMs.

6.2.8.5 About the Hidden Station Problem

A hidden station is a situation in which two wireless stations are within range of the same Access Point RLM, but are not within range of each other.

Figure 24 The Hidden Station Problem illustrates an example of the “hidden station” problem. Both station A and station B are within range of the Access Point RLM however, station B cannot “hear” station A, therefore station A is a “hidden station” for station B.

When station B starts to communicate with the Radio Link Module, it might not notice that station A is already using the wireless medium. When station A and station B send messages at the same time, they might collide when arriving simultaneously at the Access Point RLM. The collision will most certainly result in a loss of messages for both stations.

In situations as pictured Figure 24 The Hidden Station Problem, RTS/CTS medium reservation may provide a solution to prevent message collisions by handing over transmission control to the Access Point RLM.

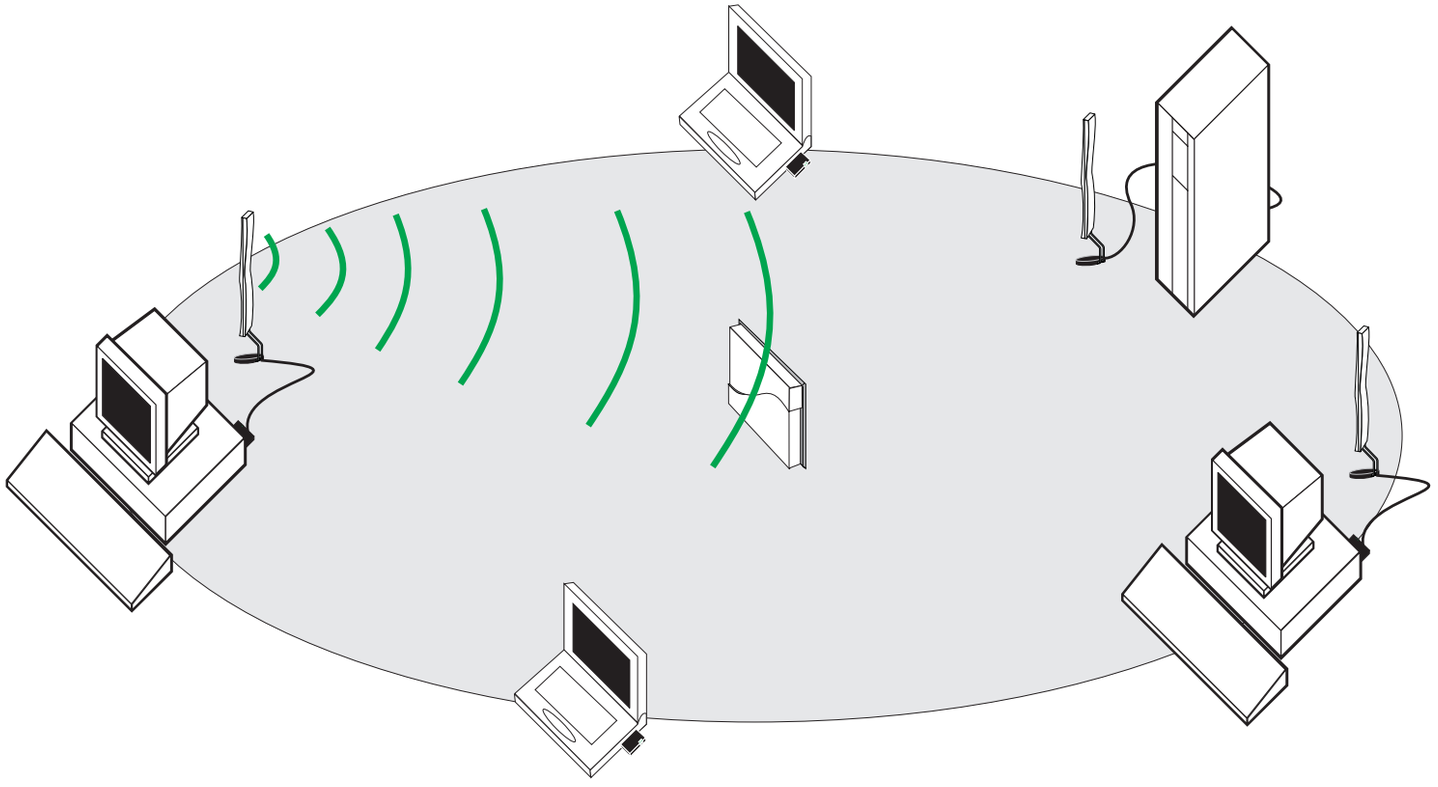
Troubleshooting a “hidden station” problem usually provides the best results when it is performed on the suspected stations that suffer from errors as a result of the “hidden station” problem.

When configuring the PC Card CP 1515 parameters of an individual station you can enable the RTS/CTS Medium Reservation parameter:

- To enable RTS/CTS Medium Reservation parameter, choose **Add/Edit configuration profile** in the CP 1515 Manager, select the **Advanced** tab and enable **RTS/CTS Medium Reservation**.

You can enable RTS/CTS Medium Reservation on individual stations, i.e. the setting of this parameter does not have to be the same for all SIMATIC NET IWL equipped devices in your network.

Figure 25 Medium Reservation “Request to Send”



6.2.8.6 About the Medium Reservation Mechanism

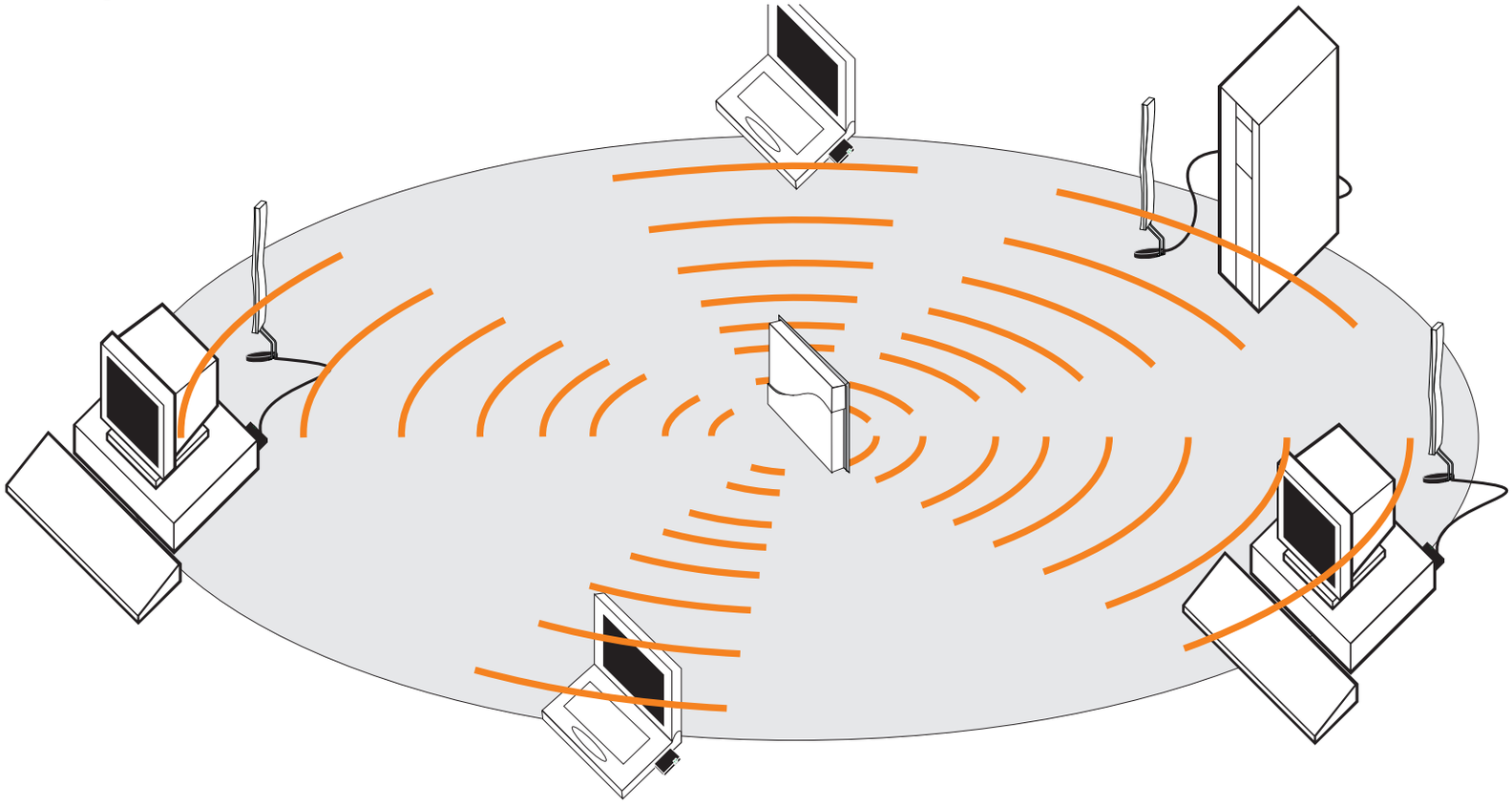
When you enable RTS/CTS medium reservation on a suspect “hidden station,” this station and its Access Point RLM will use a Request to Send/ Clear to Send protocol (RTS/CTS).

- The station will send an RTS to the RLM, that will include information about the length of the frame that the station would like to transmit (see Figure 25 Medium Reservation “Request to Send”).
- Upon receipt, the Access Point RLM will respond with a CTS message to all stations within its range to:
  - notify all other stations to defer transmissions for the time-frame of the requested transmission.

— confirm the requestor station that the Access Point RLM has checked the medium for availability, and has reserved it for the time-frame of the requested transmission.

The CTS process is shown in Figure 26 Medium Reservation “Clear to Send”.

Figure 26 Medium Reservation “Clear to Send”



NOTE:

In most networking environments it is very unlikely that you will need to enable RTS/CTS medium reservation on the Access Point RLM to prevent collisions.

Since all stations connected to the Access Point RLM are typically within range of that Radio Link Module, they should be able to sense whenever the RLM is using the medium to transmit messages via the wireless medium.

Enabling RTS/CTS medium reservation on the RLM would require the Access Point RLM to ask for a CTS for every message that it wishes to forward to stations within its range, even if it is forwarding traffic between stations that belong to the same wireless cell.

This might cause redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

If you insist on enabling RTS/CTS medium reservation on the Access Point RLM, you will notice that the configuration of this option for Access Points RLMs is slightly different from that of wireless stations.

The Access Points RLMs allow you to customize the sensitivity of the RTS/CTS mechanism. By entering a user-defined frame length value in the **RTS/CTS Medium Reservation Threshold** field (in the edit mode, select **Interface** tab, then click the **Advanced** button), you can influence when the Access Point RLM should apply the RTS/CTS mechanism. For example:

- When a message is shorter than the RTS/CTS medium reservation threshold, the Access Point RLM will not initiate an RTS to the addressed station, but use the CSMA/CA protocol: i.e. it will immediately transmit the message when it senses that the medium is free.
- When the length of a message exceeds the RTS/CTS medium reservation threshold, the Access Point RLM will first send an RTS to the addressed station and defer transmission until the addressed station has responded with a CTS message.

All other stations will defer their transmissions for the duration of the "radio-silence time" identified in the CTS message.

6.2.8.7 Enabling RTS/CTS Medium Reservation

1. Start the RLM Manager program, select the Radio Link Module that services the wireless cell where you suspect poor performance caused by a hidden station problem and click the **Edit** button.
2. Select the **Wireless Interfaces** tab.
3. Choose the socket that contains the network interface that suffers from a hidden station.
4. Click the **Advanced** button.
5. Click the **RTS/CTS Medium Reservation** check box.
6. In the **Threshold** field, enter a value in the range of 0 to 2347.

   By default, the RTS/CTS medium reservation threshold is 2347 (disabled) which means that RTS/CTS will not be used.

   - In a network using RTS/CTS medium reservation, a typical setting for the medium reservation threshold is 500.
   - Alternatively enter a value of your choice.

   The value you enter here will determine when the Access Point RLM will issue a Request to Send (RTS). For example, if the value you select is 500:

   - The RLM will send the RTS/CTS protocol for each message that exceeds the length of 500.
   - Messages with a length that is shorter than 500, will be transmitted according to the standard CSMA/CA protocol.

7. Click **OK** to return to the Interface tab.
8. Click **OK** again to save the new configuration to the Access Point RLM and to return to the main RLM Manager window.
9. Next create a backup-file of the new configuration (see Step 4 - Create a Back-up of the Configuration (page 66)).

6.2.8.8 Frequency Channel Management

When your network consists of more than one Access Point RLM, we recommend that you alternate sub-channel frequencies between adjacent Access Points RLMs to provide more bandwidth to the wireless stations in each cell.

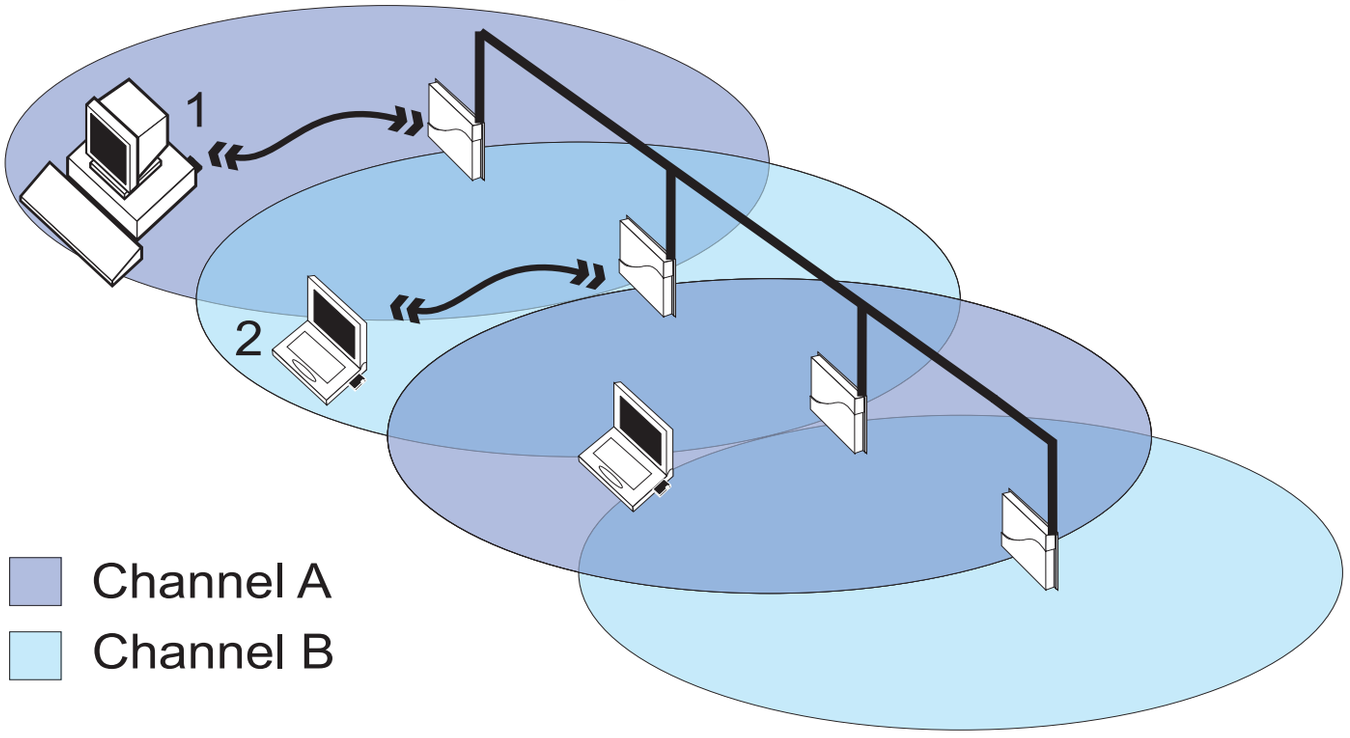
The number of available channels is subject to local radio regulations that apply in your country. A list of supported channels for your country can be found in the manual “Industrial Ethernet Wireless LAN Basics” and via the MOBIC web site **http://www.siemens.com/mobic**.

6.2.8.9 Dual Channel Configuration

A Dual Channel system could look as follows:

- All Access Point RLMs identified as operating on channel A would use channel 1 (2412 MHz).
- All Access Point RLMs identified as operating on channel B would use channel 11 (2462 MHz).

Figure 27 Dual Channel Configuration



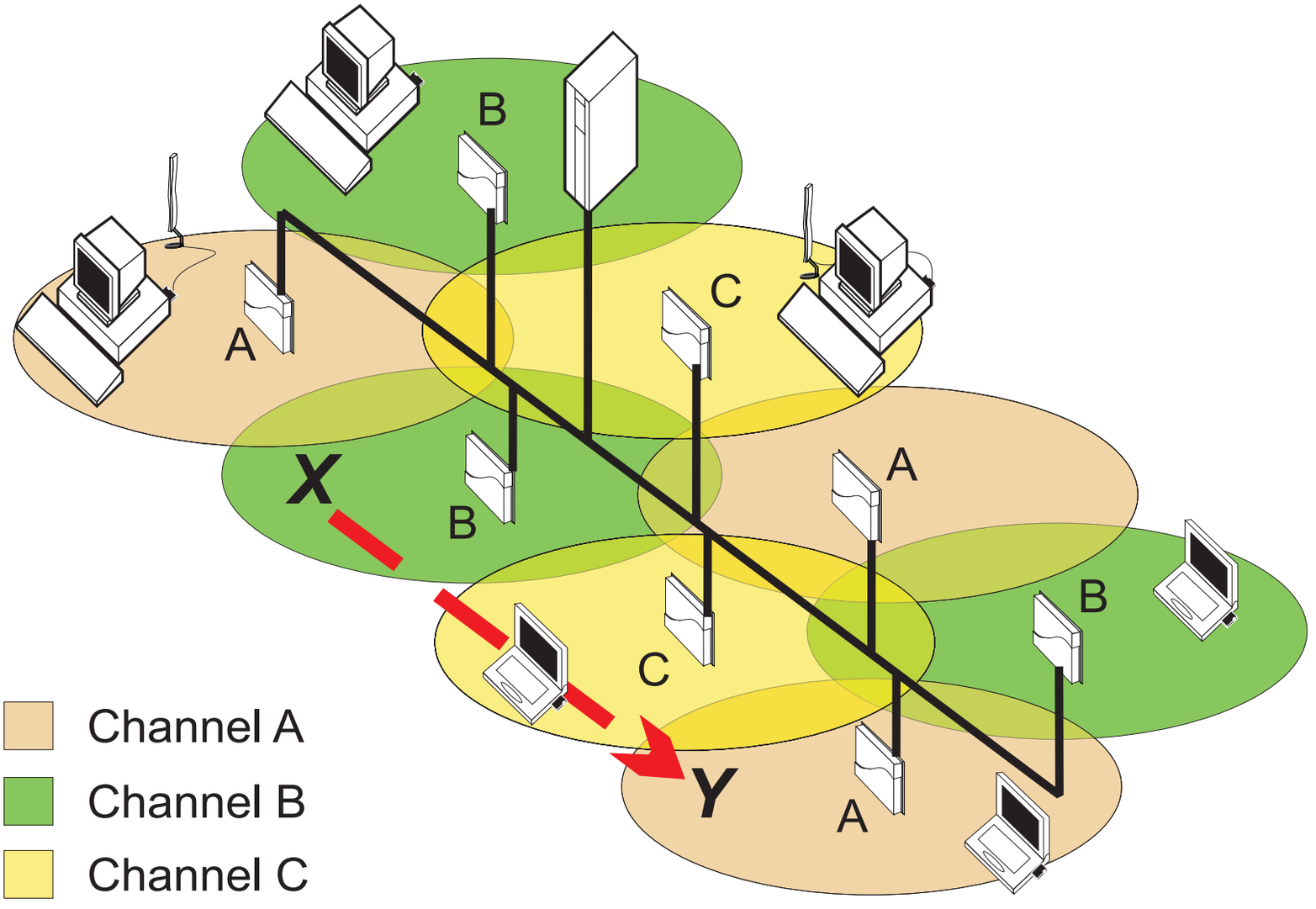
This way you can apply a maximum channel separation for neighboring Access Points RLMs that will easily satisfy the requirements recommended for optimal operation.

Station 1 would use channel A to communicate with its Access Point RLM without bothering station 2 to defer its transmissions to the neighboring Radio Link Module. When either one of the stations would roam to another location, it will automatically switch its radio to any other operating channel required to remain connected to the network.

6.2.8.10 Multiple-Channel Configuration

You can alternate the frequency channels of your Access Points RLMs between three or more sub-channels (depending on local radio regulations that apply in your country).

Figure 28 Multiple Channel Configuration



For example, looking at Multiple Channel Configuration (page 140), to set up a three channel system you could configure the Access Points RLMs as follows:

- All Access Points RLMs identified as operating on channel A would use channel 1 (2412 MHz)
- All Access Points RLMs identified as operating on channel B would use channel 6 (2437 MHz),
- All Access Points RLMs identified as operating on channel C would use channel 11 (2462 MHz)

This would just meet the minimum channel separation of 25 MHz for neighboring Radio Link Modules that is recommended for optimal operation.

A station roaming from location *X* to location *Y* would automatically switch its radio consecutively from channel A, B to C to remain connected to the network.

When your network includes RLM devices, you can use the RLM in combination with two PC Cards CP 1515 to create overlapping cells for maximum throughput performance.

In that case, you must assign different frequency channels to each card (with a separation of 25 MHz or more) to avoid cross-talk between the two cards.

6.2.8.11 Configuring Channel Frequency

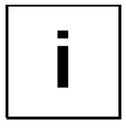
To change the frequency of your Access Point RLM, proceed as follows:

1. Connect to the RLM by opening the RLM Manager, selecting the target Access Point RLM, and click the **Edit** button.
2. Select the **Wireless Interfaces** tab.

3. Choose the socket (A or B) for the network interface that you would like to configure.
4. Click the **Advanced** button. The PC Card CP 1515 supports multiple sub-channels, a pull-down box will appear, allowing you to select a different operating frequency. The number of channels is subject to local regulations.
5. In the Wireless Advanced Setup window, use the **Channel** pull-down menu to select a sub-channel that allows for maximum channel separation from neighboring Access Points RLMs (minimum channel separation: 25 MHz).

   Table 2 lists a number of successful channel combinations that you can use to configure SIMATIC NET IWL networks with multiple Radio Link Modules.

   - For Dual Channel Configuration (page 138), alternate between channels A and B.
   - For Multiple-Channel Configuration (page 140), alternate between channels A, B and C



NOTE:

The availability of the listed channels in Table 2 Recommended Sub-Channel Configurations is subject to local radio regulations that apply in your country. A complete list of supported channels for your country can be found in the manual “Industrial Ethernet Wireless LAN CP Basics” and via the MOBIC web site **http://www.siemens.com/mobic**.

Table 2 Recommended Sub-Channel Configurations

Channel A	Channel B	Channel C
2412 MHz (1)	2437 MHz (6)	2462 MHz (11)

For wireless networks where wireless cells only have a slight overlap, you may also experiment with multiple channel configuration using a channel separation of less than 25 MHz, for example using the channels as listed in Table 3 Optional Sub-Channel Configurations.

Table 3 Optional Sub-Channel Configurations

Channel A	Channel B	Channel C	Channel D
2412 MHz (1)	2427 MHz (4)	2442 MHz (7)	2457 MHz (10)

6. Click **OK** to close the Wireless Advanced Setup window and return to the **Wireless Interfaces** tab.
7. (Optional) Repeat steps 3-6 to verify and/or change the frequency for the second network interface in this Access Point RLM.
8. Click **OK** again to save the new configuration to the Radio Link Module and to return to the main RLM Manager window.
9. Next create a backup-file of the new configuration (see Step 4 - Create a Back-up of the Configuration (page 66)).
10. Update the "Access Point Configuration Record" in chapter A "Start-up Configuration" to reflect these changes.

11. (Optionally) Modify the configurations of all your other Access Points RLMs accordingly. We recommend that you use different frequencies for neighboring Radio Link Modules, as described in Dual Channel Configuration (page 138) or Multiple-Channel Configuration (page 140).

6.2.9 Link Integrity

In situations where the connection of the Access Point RLM to the rest of the Ethernet network fails, typically as a result of a broken cable connection or network error, the Ethernet failure might disrupt regular network communication for (roaming) wireless stations.

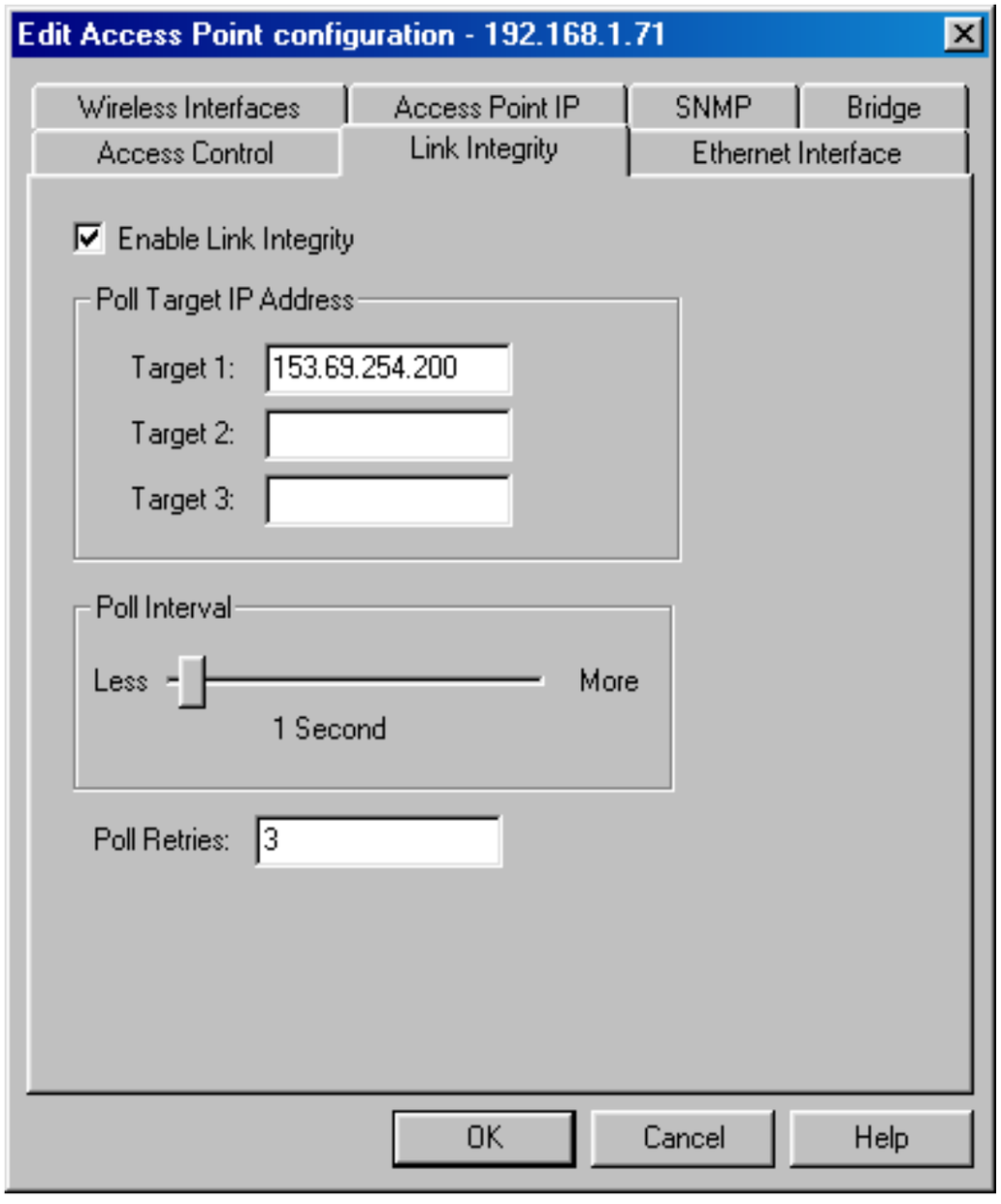
CAUTION:
This feature is only used if your network provides duplicate Ethernet connections.

If the wireless connection however is still intact, the wireless station would not roam to another Access Point RLM, since its radio might still interpret its "physical" connection to the Access Point RLM as "good" or "acceptable."

The Ethernet link integrity feature is a high-end solution that enables you to resolve this type of network failures, as it allows Access Points RLMs to:

- Detect any disruption in its connection to network services by testing the link between the RLM and a maximum of three IP hosts.
- Reconnect automatically to another Access Point RLM in situations where disruptions occur that are not related to poor radio communications.

Figure 29 Link Integrity Window



For more information about link integrity refer to the help-file of the RLM Manager program.

6.3 Designing High Capacity Networks

In networking environments where you have either data intensive users, or a large number of users in a small area, you may wish to improve the throughput efficiency and/or load balancing of your Access Points RLMs.

This solution described in this section allows you to balance “maximum range for minimum hardware investments” versus “maximum throughput performance for higher hardware investments.”

6.3.1 About the CSMA/CA Protocol

In normal network configurations, all equipped devices apply a standard mechanism to avoid collision of wireless messages. When a station intends transmitting a message, it will first sense whether no other station is already transmitting (“using the wireless medium”).

- If no other transmissions are sensed, the station will start its transmission.
- If it does sense another transmission carrier, the station will apply a random defer timer. After the timer has expired it will start sensing the medium again to see if it can start transmitting.

This protocol, also referred to as the “Carrier Sense Multiple Access/ Collision Avoidance” (CSMA/CA) protocol works fine in most networking environments. The user of a wireless computing device will hardly notice the deferral behavior of the wireless radio.

In network environments with many wireless users in the vicinity of one another and/or wireless stations that are engaged in heavy data traffic, you

may perceive that wireless stations show a degrading performance, perceived as long network response times when communicating via the network.

Where poor performance is typically caused by poor radio link quality (identified by a poor signal to noise ratio (SNR)), the scenario described above may also be perceived in areas where:

- Site monitor measurements show an excellent wireless coverage by at least two Access Points RLMs or more on every location.
- Link test measurements at such locations may show:
  - An excellent SNR for communications between wireless stations and the Radio Link Module.
  - A large number of messages transmitted at lower rates.

In this type of situations the disappointing network performance might be caused by the busy wireless traffic in that area, where the CSMA/CA protocol causes the wireless stations to defer transmissions to often for either:

- Heavy data traffic by other stations in the same wireless cell
- Traffic from stations in neighboring cells, where stations in a location where wireless cells overlap one another seem to suffer more than the other stations.

The last example would typically occur only in networks where all Access Points RLMs have been configured to operate at the same frequency, or at frequencies with an insufficient channel separation (see Frequency Channel Management (page 138)).

6.3.1.1 Influencing the Deferral Behavior

To overcome the performance issue described on previous pages, you can choose to design a high performance network based on the following principles:

- Add more Radio Link Modules to your network.
- Configure Access Points RLMs in neighboring cells to operate at different frequency channels with a maximum channel separation (see Frequency Channel Management (page 138)).
- Adjust the **Distance Between APs** parameter to optimize the load balance of the number of wireless stations per Access Point RLM (see Distance Between APs (page 194)).

CAUTION:

Distance between APs is a parameter that must be set on both the wireless stations and the Access Point RLM. The values that you select must be the same for ALL wireless equipped devices in your network to avoid unpredictable behavior of your network and the roaming connectivity of wireless devices.

By changing the **Distance between APs** parameter from **Large** to **Medium** or **Small**, you can virtually reduce the receiver sensitivity of the wireless radios, that will show the following behavior:

- The stations will show a more active roaming behavior and connect to one of the added Access Points RLMs more quickly.

- Considering the fact that you have added more Access Points RLMs, the deferral behavior does no longer need to be as strict in environments where the density of installed Radio Link Modules was fairly low:
  - The stations will only defer transmissions when the signal level of a message sensed on the wireless medium equals or exceeds a specific level.
  - Messages with a low signal level are not likely to be addressed at the Access Point RLM that services the local cell, since the more active roaming behavior should have caused the station to connect to another RLM.

To support the more active roaming behavior of the wireless stations and to compensate the lower receiver sensitivity, changing the Distance between APs parameter should correspond with the actual increase of and more dense placement of your Access Points RLMs.

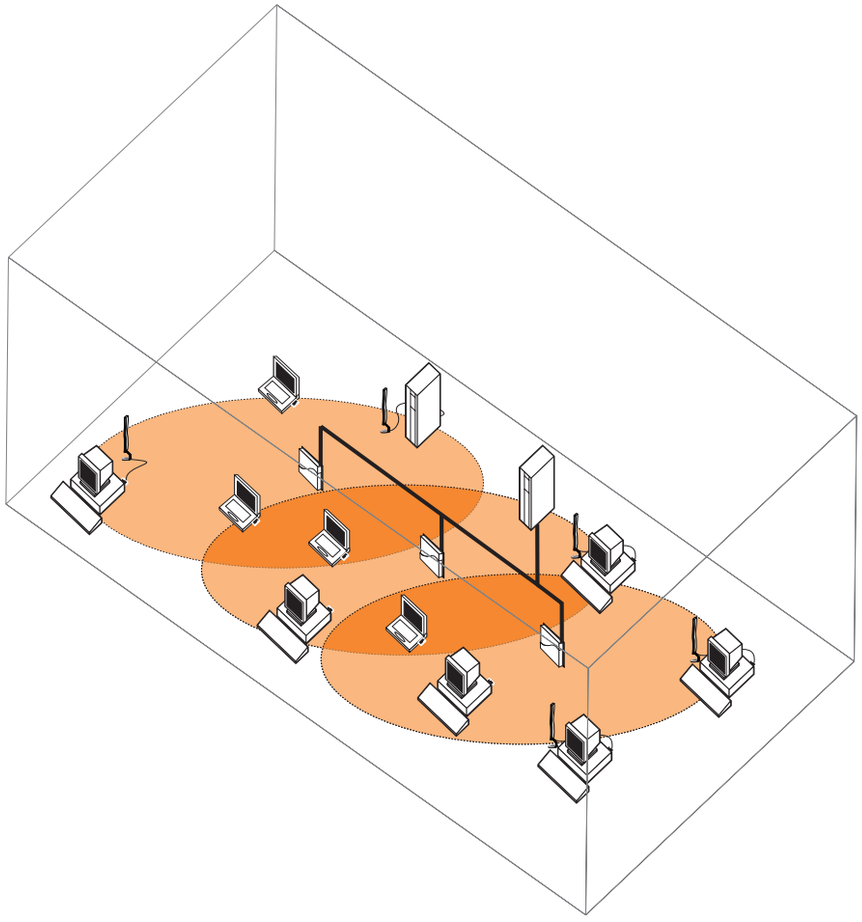
The examples listed on the following pages will illustrate the effect of the various Distance between APs configurations.

In Figure 30 Large Distance between APs you see the standard configuration of networks, where **Distance between APs** parameter has been set to **Large**.

- The receiver sensitivity in this mode causes the wireless radio device to defer transmissions for all messages that it senses within its range (identified by the colored circles).
- Roaming stations in a specific cell will remain connected to the servicing Access Point RLM until they exit the wireless cell.

This setting provides you with the maximum radio range possible with the minimum number of Radio Link Modules to cover the wireless network area.

Figure 30 Large Distance between APs



The examples in Figure 31 Medium Distance between APs and Figure 32 Small Distance between APs show you the effect of changing the Distance between APs parameter. Although the absolute range of the wireless radio is still the same, the Distance between APs setting has virtually reduced the range of the wireless cell by applying different levels of receiver sensitivity:

- The absolute range of the radio signal from the Access Points RLMs is identified by the gray-dotted circles
- The reduced virtual range is identified by the colored areas.

With the new settings for the Distance between APs parameter, stations will only defer for radio signals that are received at a level that is equal or higher to the average signal as applicable in the colored areas. Messages with a lower signal level are considered to be traffic belonging to another cell, so will be ignored when the station determines whether it can start transmitting.

Roaming stations will start looking for/connect to another RLM as soon as they leave the colored area belonging to a specific Access Point RLM.

Figure 31 Medium Distance between APs

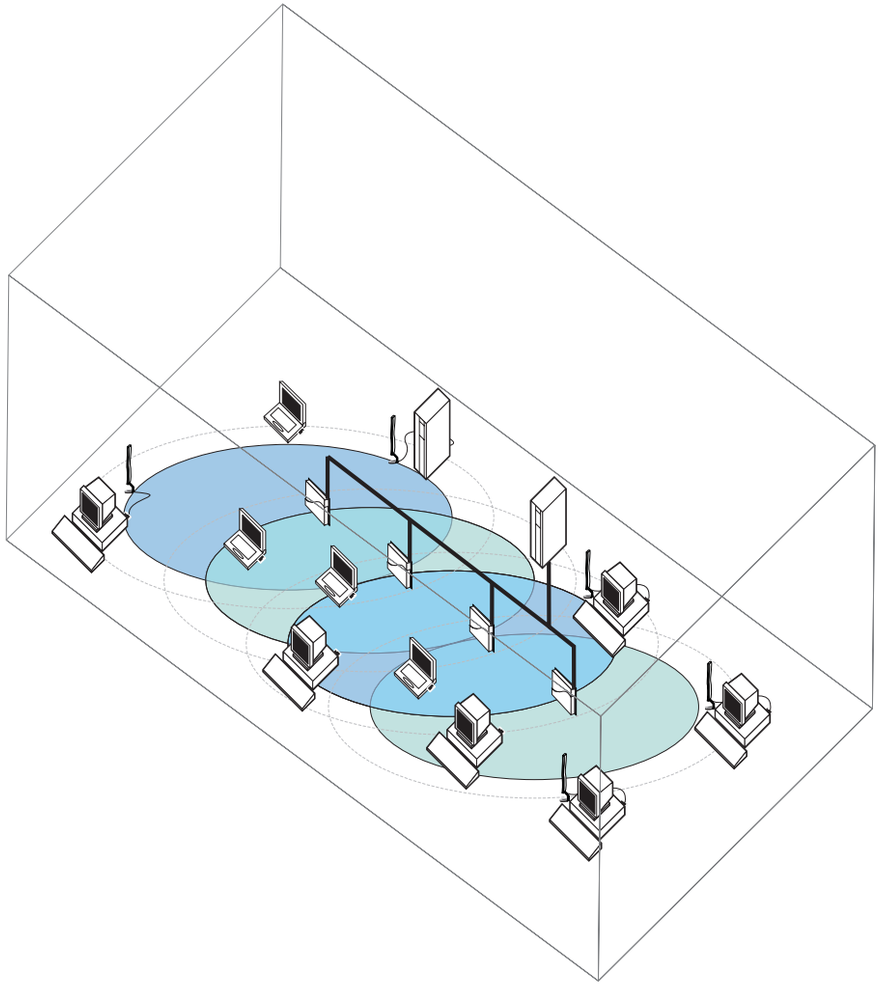
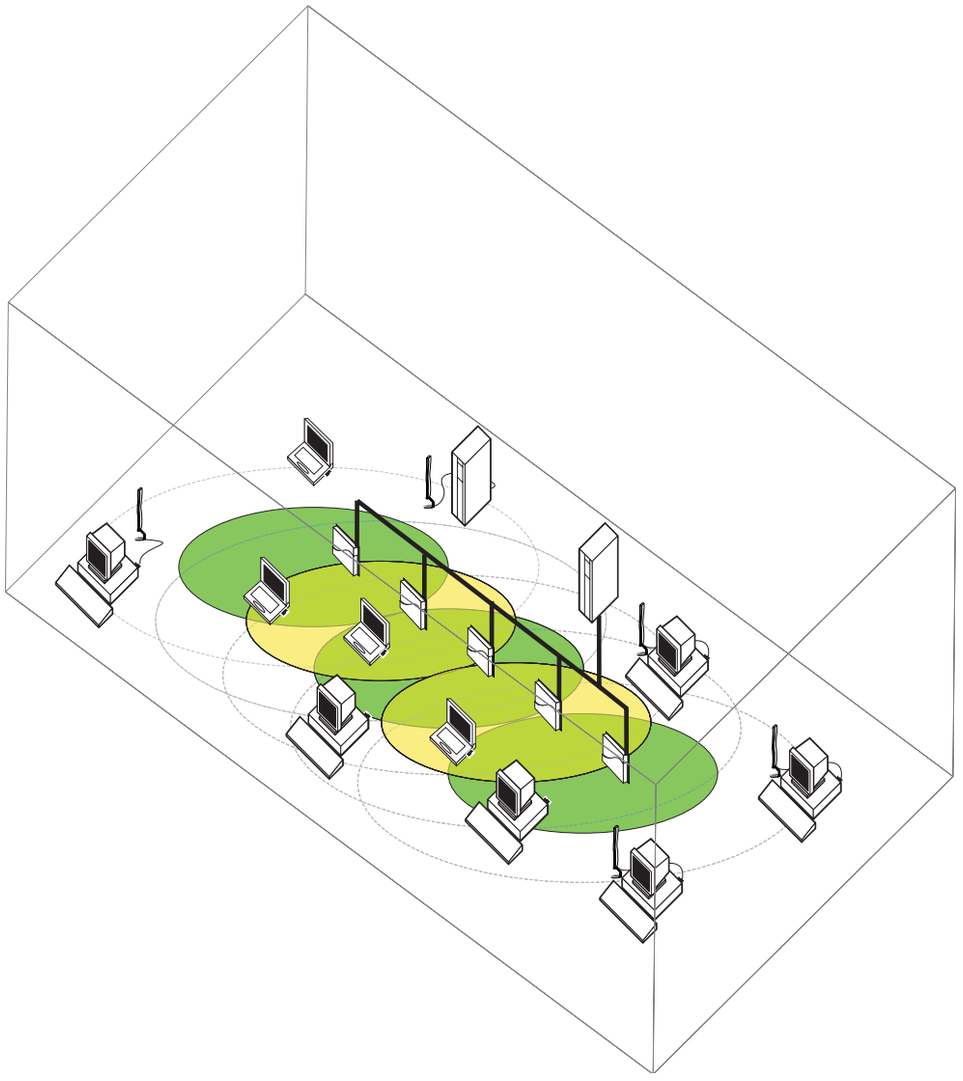


Figure 32 Small Distance between APs



7 Security

7.1 Introduction

An advantage of the IEEE 802.11 standard for wireless networks is that it gives a quick and easy way to connect your wireless station to a network. For instance, wireless stations that have been configured with the network name “ANY” will connect to the first IEEE 802.11 compatible Access Point RLM it can find within range.

The drawback of this “quick & easy connectivity” is the vulnerability of the LAN to unauthorized access. Does this mean that Wireless LANs are not secure? The answer is no:

- Access to network resources is controlled via standard security mechanisms, such as user names and passwords,
- The Siemens SIMATIC NET Industrial Wireless LAN products allow you to apply additional security measures to restrict access to your wireless medium and/or network resources.

Subject to the level of security required in your network environment, these measures may include:

- Securing Access to Wireless Data (page 155).
- Wireless Data Encryption (page 167).
- Securing Access Point RLM Setup (page 177).
- Advanced Security Maintenance (page 183).

7.2 Securing Access to Wireless Data

To prevent unauthorized stations from accessing data that is transmitted over the network, the products support the following levels of security:

- "Restrict Wireless Access to the Network"
- Data encryption to encrypt all data transmitted via the wireless medium (see Wireless Data Encryption (page 167)).

These security measures that apply to communications at the "physical layer" complement the "user name/password" validation at the "network layer" as implemented by standard network operating systems.

7.2.1 Restrict Wireless Access to the Network

To exclude unknown and unauthorized computing devices from establishing a wireless connection to the network, you can use the following options:

- Closing your network to all stations that have not been programmed with the correct network name (see Closing the Wireless Network (page 156)).
- Use access control tables to build a list of authorized stations allowed to establish a wireless connection with the network (see Access Control (page 159)).

7.2.2 Closing the Wireless Network

Closing the wireless network prevents unauthorized users from accessing the Access Point RLM within a specified SIMATIC NET Industrial Wireless LAN network. If a user tries to access the network, without configuring their station with the correct network name, the station will not be able to bridge data on the RLM.

There are two options for this type of access security: **Open** and **Closed**.

- The **Open** configuration is the standard IEEE 802.11 mode that will allow access to the Access Point RLM for:
  - all stations with the correct network name.
  - all stations with the network name set to "ANY."
- The **Closed** configuration is the Siemens SIMATIC NET Industrial Wireless LAN proprietary mode that closes your network to all stations that have not been programmed with the correct network name.

  This option will deny access to:
  - all SIMATIC NET IWL stations with the network name set to "ANY" and,
  - all non-SIMATIC NET IWL stations with a "zero string SSID" or "ANY" as network name.

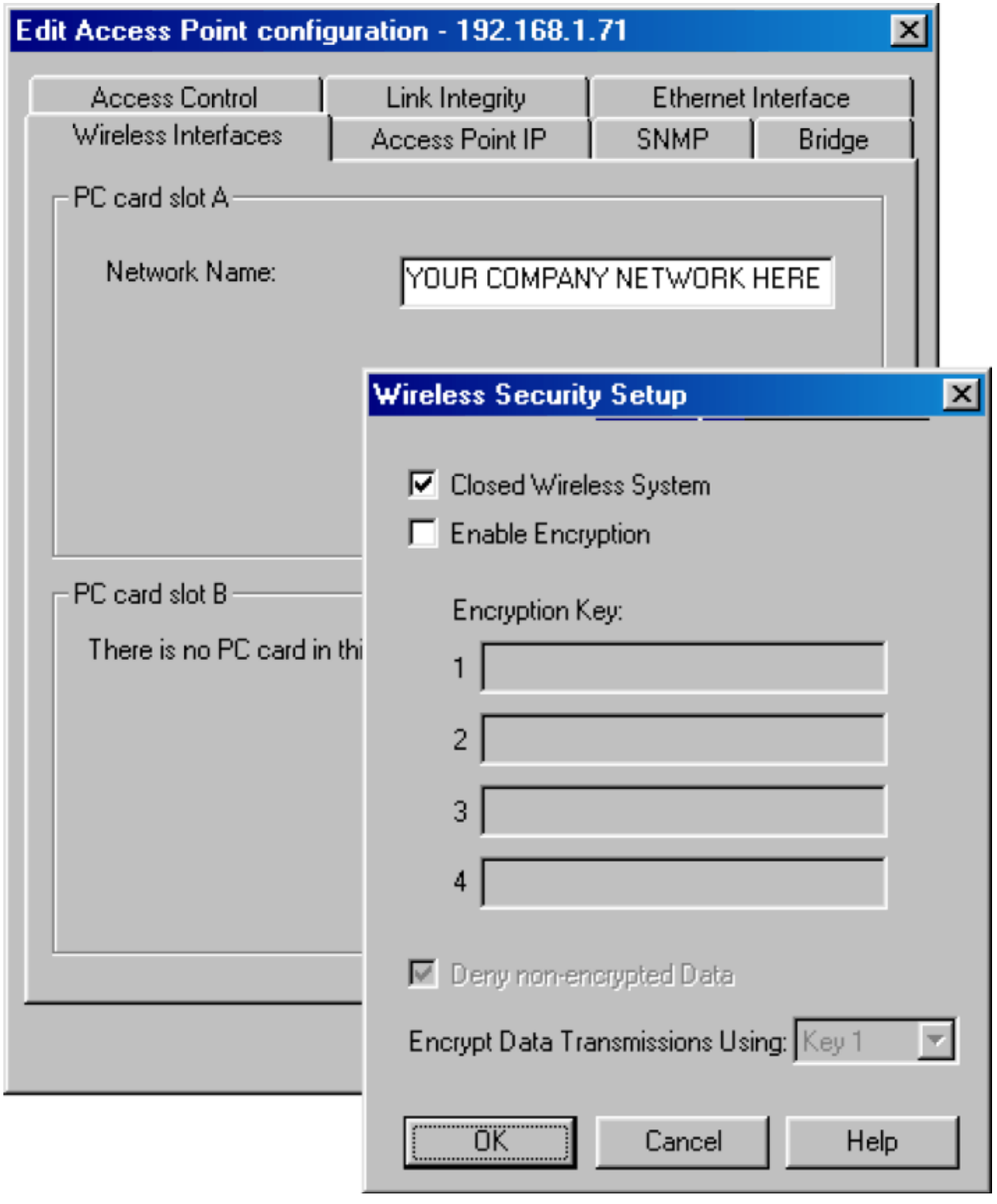
NOTE:

The **Closed** option is not compliant with the IEEE 802.11 standard for wireless LANs.

To close your network proceed as described below:

1. Start the RLM Manager and select the Access Point RLM.
2. Click **Edit** to connect the RLM.
3. Select the **Wireless Interfaces** tab (see Figure 33).
4. Select the interface (**PC Card slot A** or **B**) of the network you wish to secure.
5. Click the **Security** button to display the security properties.
6. Click the check box next to **Closed Wireless System**.
7. Click **OK** to confirm and close the Wireless Security Setup window.

Figure 33 Close the Wireless System



8. (Optional) Click the second interface to set the security parameters (return to step 4).

9. Click **OK** to save the new configuration to the Access Point RLM and to return to the main RLM Manager window.

WARNING:
Your Access Point RLM will automatically reboot and start bridging operation again allowing access only to those users that have been configured with exactly the same network name as identified in the setup of your Access Point RLMs.

Repeat steps 1 through 9 for all other Access Points RLMs.

7.2.3 Access Control

Another method to restrict wireless access to the Radio Link Module is to use the access control table feature and/or the RADIUS Server Access Control feature.

If you decide to enable the access control table feature your RLMs will:

- only bridge messages to/from authorized stations, that have been identified in the access control table.
- ignore all requests to forward data to/from non-listed SIMATIC NET Industrial Wireless LAN stations.

Enabling access control is a more rigid security mechanism than “Closing the Wireless Network”, as it requires the LAN administrators to authorize each individual Wireless LAN station.

To authorize wireless stations to access the network, the LAN administrator(s) must:

- append the unique universal MAC address of the Wireless LAN station to the access control table file (*.tbl), and
- upload the access control table file to all RLMs.

NOTE:

The access control feature does not work in network environments that require local MAC addressing.

If you decide to enable RADIUS Access Control, you can:

- Specify the lifetime of a granted authorization
- Set the authorization password
- Assign up to two RADIUS servers for validating the MAC address of wireless stations.

To enable RADIUS Server Access Control refer to Enabling RADIUS Server Access Control (page 165)

7.2.4 Enabling Access Control

To enable access control you will first need to create an access control table file (*.tbl) using the RLM Manager program.

You can upload the access control table file into all Radio Link Modules in your network as part of a (new) configuration (see Importing an Access Control Table (page 163) for more information).

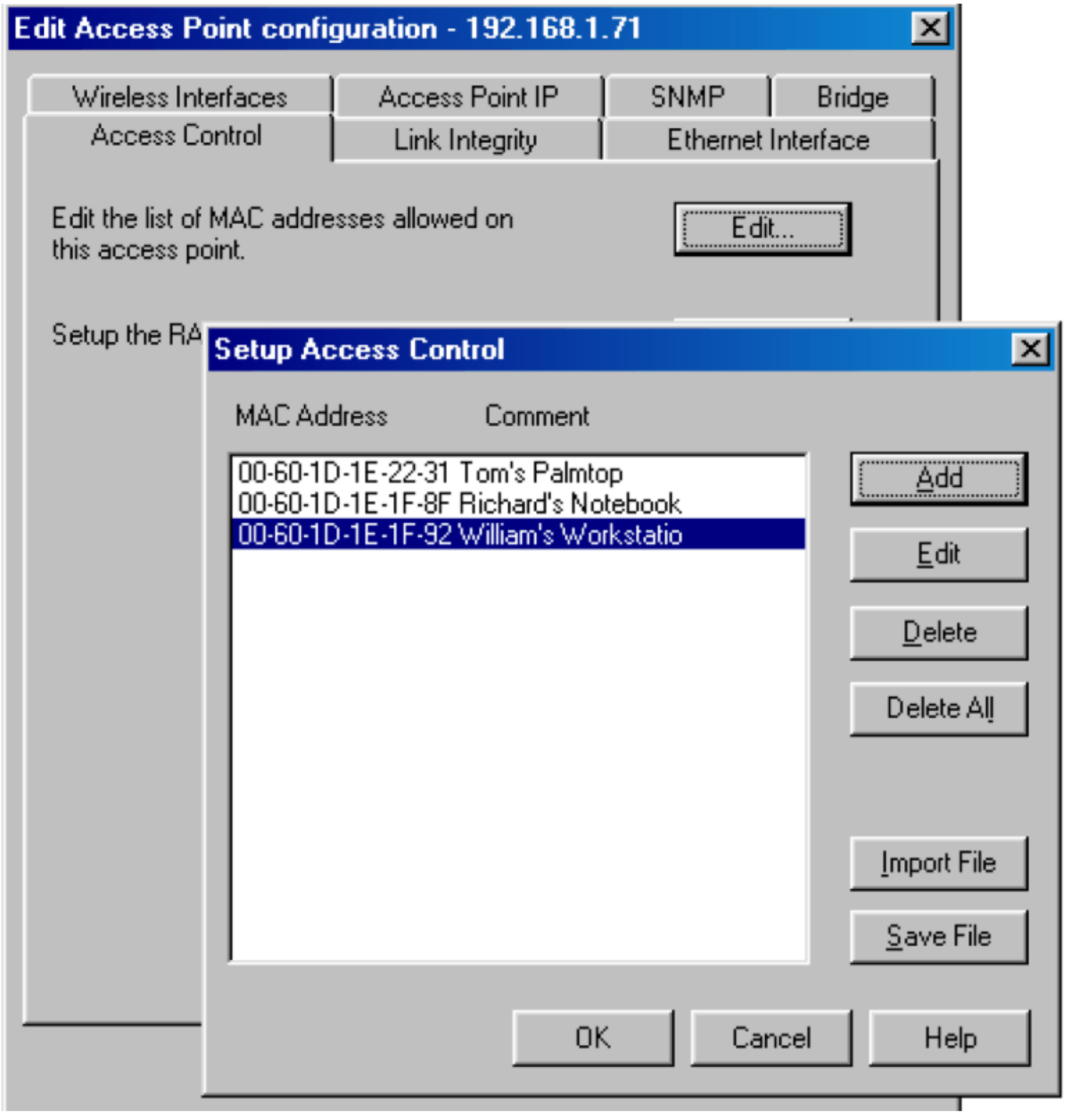
7.2.5 Creating/Editing an Access Control Table

To create or edit the access control table:

1. Start the RLM Manager and select the Radio Link Module.
2. Click the **Edit** button.
3. Select the **Access Control** tab.
4. Click the **Edit** button to display all MAC addresses that are currently authorized as pictured in Figure 34 Setup Access Control.

   By default, access control is set to **<All will be permitted>**, i.e. there are currently no access restrictions defined.
5. Use the following buttons to modify the MAC address table:
   - **Add** - to add MAC addresses one at a time. You can also use the **Comments** field to enter a name or add a comment about the listed MAC address.
   - **Edit** - to change entries in the table.
   - **Delete** - to remove MAC addresses one at a time.
   - **Delete All** - remove all MAC addresses and disable access control.
   - **Import File** - to import an existing access control table.
   - **Save File** - to save the current access control to a file.
6. Repeat step 5 for all stations you want to authorize to send/receive data via this RLM.

Figure 34 Setup Access Control



7. Click the **Save file** button to make a back-up copy of the access control table file you just created (*.tbl).

   You can use this file later to import the configuration into other Access Point RLM.
8. Click **OK** to return to the Access Control tab.
9. Click **OK** again to save the new configuration to the RLM and to return to the main RLM Manager window.
10. (Optional) Save the configuration to a local back-up file (*.cnf) as described in Step 4 - Create a Back-up of the Configuration (page 66).

To save the table to RLM, please refer to Importing an Access Control Table (page 163)[1].

7.2.6 Importing an Access Control Table

To import an access control table file (*.tbl) to your Radio Link Modules:

1. Start the RLM Manager and connect to the Access Point RLM in the edit mode.
2. Select the **Access Control** tab and click the **Edit** button to display all MAC addresses that are currently authorized.
3. Click the **Import File** button and select the access control table file (*.tbl) that you wish to import.
4. Click the **Open** button to import the selected file.
5. Click **OK** to return to the **Access Control** tab.

1. Also refer to information on Common Parameters (page 219).

6. Click **OK** again to save the new configuration to the Radio Link Module and to return to the main RLM Manager window.
7. (Optional) Save the configuration to a local back-up file (*.cnf) as described in Step 4 - Create a Back-up of the Configuration (page 66).

7.2.7 Disabling Access Control

To disable access control for your Radio Link Modules:

1. Start the RLM Manager and connect to the Radio Link Module in the edit mode.
2. Select the **Access Control** tab and click the **Edit** button to display all MAC addresses that are currently authorized.
3. To disable access control, click the **Delete All** button. The MAC address window will read **<All will be permitted>**.
4. Click **OK** to return to the **Access Control** tab.
5. Click **OK** again to save the new configuration to the RLM and to return to the main RLM Manager window.
6. (Optional) Save the configuration to a local back-up file (*.cnf) as described in Step 4 - Create a Back-up of the Configuration (page 66).
7. Update the “Access Point Configuration Record” to reflect this change.
8. (Optional) Modify the access control settings for all other Radio Link Modules.

7.2.8 Enabling RADIUS Server Access Control

RADIUS Server Access Control is a method where you use Radio Link Modules in combination with a third-party RADIUS server.

To use RADIUS Server Access Control, you will need to:

1. Setup a RADIUS server

2. To configure a RADIUS server do the following:
   - The list of MAC addresses should be entered in the server's "users" file/database along with the password (=authorization password).
   - It is also necessary to build a list of IP addresses of all Radio Link Modules that will use the RADIUS server. This list should be entered in the server's station file/database along with the authorization password.
3. Build a list of MAC addresses of all (wireless) stations that you wish to authorize to establish a wireless connection with your Radio Link Module infrastructure.
4. Configure all Radio Link Modules to:
   - Enable RADIUS MAC Address authentication
   - Set the RADIUS Authorization Lifetime
   - Set the Authorization Password
   - Identify the IP Address of the RADIUS server(s)
   - Verify the Authentication Port of the RADIUS server(s)

7.2.8.1 RADIUS Server Access Control

RADIUS Access Control enables you to:

- Specify the lifetime of a granted authorization
- Set the authorization password
- Assign up to two RADIUS servers for validating the MAC address of wireless stations.

For each RADIUS server you will need to specify:

- The unique IP address of the RADIUS server
- The Authentication port as used by the selected server.

To restrict access to your network using MAC address control via a RADIUS server:

1. Start the RLM Manager and select the Acess Point RLM.
2. Click the **Edit** button.
3. Select the **Access Control** tab.
4. Click the lower **Edit** button to display the RADIUS server name and secret parameter.
5. Enable the check box **Enable RADIUS Server**.
    - Default value is: RADIUS Access Control Disabled

For more information refer the help-file (press F1) of the RLM Manager.

7.3 Wireless Data Encryption

To provide the highest level of security to wireless data transmitted via your wireless network, you can use the Wired Equivalent Privacy (WEP) data encryption.

To use WEP data encryption in your network, you need:

- All wireless stations and access points must be equipped with CP 1515 cards
- All devices must be configured with matching WEP encryption key values.

WEP data encryption uses 13-character encryption keys, based on the RC4 encryption algorithm, that will be used to encrypt/decrypt all data transmitted via the wireless interface.

You can specify up to 4 different keys to *decrypt* wireless data, and select one of the specified decryption key values to *encrypt* wireless data.

The option to use 4 different keys for decrypting wireless data, allows you to change your WEP keys at regular intervals without affecting regular network performance (see also Maintaining WEP Encryption Keys (page 183)).

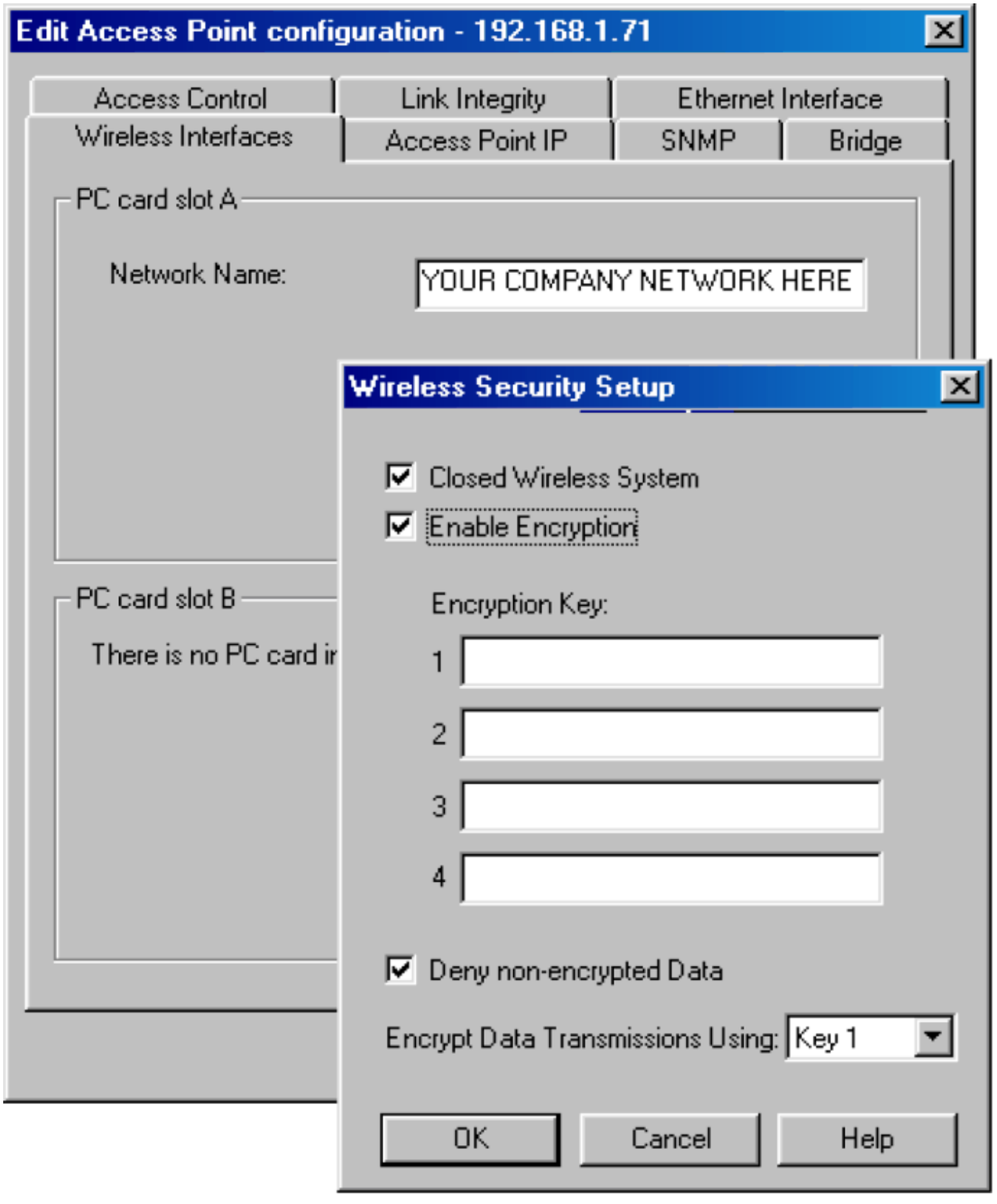
7.3.1 Enabling WEP Encryption

To enable WEP encryption you will need to ensure that:

- All wireless devices have been equipped with CP 1515 cards
- All wireless devices will be configured with matching encryption key values.

You are advised to use the Radio Link Module configuration log to write down the proposed WEP key values, and store the information in a safe place.

Figure 35 Enabling WEP Encryption



Wireless Data Encryption

Wired Equivalent Privacy (WEP) data encryption enables you to encrypt all data that will be transmitted via the wireless LAN medium.

To use WEP within your network, all access points and wireless stations must be equipped with CP 1515 cards that have been configured to use identical encryption keys.

To enable encryption:

1. Start the RLM Manager and select the RLM.
2. Click the **Edit** button.
3. Select the **Wireless Interfaces** tab.
4. Click the **Security** button to view the Wireless Security Setup window (see Figure 35 Enabling WEP Encryption).
5. Select the option **Enable Encryption** to enable encryption, and:
   - Enter up to 4 different keys to decrypt data received via the wireless interface
   - Select one of these keys to encrypt wireless data that is to be transmitted via the wireless interface.
6. Click **OK** to return to the **Wireless Interfaces** tab.
7. Click **OK** again to save the configuration to the Radio Link Module and to return to the main RLM Manager window.

WARNING:
The RLM will now reboot.

Optionally you can choose to configure your Access Point RLM to allow or deny non-encrypted data.

7.3.1.1 WEP Encryption Key Values

If you select to enable encryption you may choose to enter up to the following encryption keys.

For the CP 1515 that supports 128-bit RC4 encryption algorithm valid values are either:

- 13-digit alphanumerical value in the range of “a-z” and “0-9”
  Example: SECURE1234567
- A 26 -digit hexadecimal value, preceded by the characters “0x” (zero x).
  Example: 0x1234567890ABCDEF1234567890
- As an option, you can also use short (example 64-bit) values

Hexadecimal strings that are not preceded by the leading “0x” will be interpreted as alphanumerical string.

NOTE:

The WEP key values you enter will remain visible only when you enter the character strings. As soon as you close the Security Setup window, the values will be stored in hidden characters: i.e. a next time the Security Setup window will be displayed, you will not be able to read the WEP key values anymore. You are advised to write down the values you enter, prior to closing the window.

7.3.1.2 WEP Transmit Key value

If you enable WEP encryption, you can select one key for wireless data transmissions from the list of WEP encryption key values. You can only select a transmit key that has a correct WEP encryption key value assigned.

In case you specified no more than 2 key values, you can only select the transmit key from these two values.

CAUTION:
If you cleared the "Deny non-encrypted Data" tick box, your RLM may also transmit in "non-encrypting mode".

7.3.1.3 Deny non-encrypted Data

If you decide to use wireless data encryption, you are advised to encrypt all data that will be transmitted via the wireless medium.

In some cases however you may wish to choose to allow the Radio Link Module also to process non-encrypted data as well.

Examples of such situations could be:

- Network environments that include both wireless stations equipped with cards (CP 1515) that support WEP Encryption and cards that do not support encryption.
- Network environments where you are about to install a large number of wireless stations, using "out-of-the-box" configurations, which by default will have encryption disabled.

If you would start-up such stations with their default configuration, these stations would not be able to establish an initial connection to the network, since they wouldn't be able to interpret the encrypted beacon messages.

For optimal security against unauthorized access to your network, you are advised always to leave the **Deny non-encrypted data** option enabled (=default).

CAUTION:
Only when you would have good reasons to decide otherwise, you could clear this check-box, to allow the RLM to communicate with wireless stations that either support WEP encryption or not, or have the WEP encryption enabled or disabled.
Please read the information described in the following section prior to clearing the Deny non-encrypted Data tick box.

7.3.1.4 How WEP Encryption works

The IEEE 802.11 standard on wireless LANs was designed to provide an easy to use, and easy to install wireless network, that would allow users to combine wireless LAN products from different vendors.

The drawback of easy access and interoperability is the vulnerability to unauthorized access to and/or use of your network. Although WEP encryption provides a good way to secure access to your wireless data, there are a few things you need to know to ensure your network provides the right level of security.

When you enable WEP encryption there are two modes of WEP operation:

- Enable encryption & deny non-encrypted data
- Enable encryption & allow non-encrypted data

For optimal security, you are advised always to use the **Deny non-encrypted data** option (=default).

7.3.1.5 Enable Encryption & Deny non-encrypted Data

When you select to enable encryption and deny non-encrypted data, your Radio Link Module will:

- Only process messages received at its wireless interface, when the messages have been encrypted with either one of the four identified keys.
- Always transmit wireless data using the selected WEP key.
- Also encrypt all its multicast and broadcast traffic that it will transmit to the wireless medium.

If your network includes wireless stations configured with a non-matching WEP key, or equipped with PC Cards that do not support WEP encryption, such stations will not be able to establish a wireless connection because they will not be able to understand (decrypt) crucial network information.

7.3.1.6 Enable Encryption & Allow non-encrypted Data

When you select to enable encryption, but you cleared the **deny non-encrypted data** check box, the RLM will:

- Process all messages received at its wireless interface, regardless whether the messages have been encrypted with one of the identified keys or not.
- Encrypt wireless transmissions based on the encryption settings of the addressed station.
- If the addressed station does use WEP encryption, the Radio Link Module will send the message in encrypted format, using the selected transmit key value.

- If the addressed station does not use WEP encryption, the Access Point RLM will send the message in non-encrypted format.
- If the data message is a multicast or broadcast message, typically addressed to "all stations", the Radio Link Module will send the message in non-encrypted format.

This behavior of the Radio Link Module is not related to the way the wireless message was received at the RLM. If for example a wireless station that uses WEP encryption wishes to send data to another station in the same wireless cell, the data transmission will:

- Go encrypted from the WEP station to the RLM
- Go un-encrypted from the Radio Link Module to its final destination, if the addressed station does not support WEP encryption, or does not have the WEP option enabled.

CAUTION:

For most network environments that require a higher level of security than the standard security mechanisms supported by SIMATIC NET Industrial Wireless LAN and most of today's network operating systems (e.g. user names and passwords), Siemens advises against using this option, unless you want to provide easy access for any client station and/or migration is more critical to your data network than top-level security.

7.3.1.7 Good Practice Administering Encryption Keys

Like with other properties, your WEP lock is as safe as locking the door to your house: i.e. if you don’t stick to secure policies on who will be allowed to use the key, or will know where to find it, even the strongest lock can be opened by an intruder.

That's why, for example you wouldn't “hide” the key to your house underneath the doormat. Similar good practice should be applied to the keys you will use to encrypt wireless communications.

To minimize the risk that intruders might be able to retrieve the WEP key values you are advised to:

- Lock away any paper registration sheet that you use to define/remember the defined WEP key values.
- Change the WEP encryption key values at regular intervals on both stations and Radio Link Modules.

The option to enter up to 4 different keys to decrypt data received via the wireless interface, enables you to define a WEP key roll-over scheme.

For example you could choose to select another transmit key every x weeks, until you reach the fourth key. At that point in time you could enter 3 new WEP key values for the first three WEP key entries, prior to the expiration period of the fourth key value. Once all stations and Radio Link Modules have been set to use the first new key again, you can replace the fourth key value with a new WEP key value.

7.4 Securing Access Point RLM Setup

Security measures, such as access control, become ineffective when unauthorized persons can view and modify the configuration of your Radio Link Modules.

To protect your network configuration from undesired modifications, you are advised to implement the following measures:

- Read and read/write passwords
- SNMP IP address access list
- Trap host alert mechanisms (optional)

7.4.1 Read and Read/Write passwords

To restrict access to the Access Point RLM configuration information, you can create two authority levels for passwords:

- Read password
- Read/write password

7.4.1.1 Read password

A read password will only provide access to the Radio Link Module to monitor diagnostic information found under **Monitor** button in the main RLM Manager window.

You can define a read password in the field **Read Password** on the **SNMP** tab (Select Access Point RLM from list, click **Edit** and select **SNMP** tab). The default value is “public”.

7.4.1.2 Read/Write password

A read/write password will provide you with full access to display Radio Link Module diagnostic information found under the **Monitor** button, as well as the configuration settings found under the **Edit** button.

Entering an incorrect password will result in a time-out error, or "SNMP error no such name."

To define a read/write password:

1. Start the RLM Manager and select the target RLM from the list or enter a specific IP address.
2. Click the **Edit** button to connect to the Radio Link Module.
3. Select the **SNMP** tab.
4. In the field **Read/Write Password**, enter the new password. The default value is "public."
5. Click **OK** to save the configuration to the Radio Link Module.

WARNING:
The RLM will now reboot.

7.4.2 SNMP IP Access List

In addition to the read and read/write passwords, you can restrict access to the Radio Link Module configuration to a limited number of authorized stations.

To authorize the SIMATIC NET Industrial Wireless LAN management station to access your Radio Link Modules, you must identify:

- the unique IP address of the management station, and
- the RLM interface (port) via which this station will access the configuration

If you wish to authorize multiple stations, you can identify a range of IP addresses that you will reserve for authorized LAN administrator stations.

NOTE:

When using the SNMP IP access list, you should include the IP address of all stations that will need to retrieve configuration or diagnostic information of the Radio Link Module, i.e. stations of administrators who use either read or read/write passwords.

When the IP address or interface does not match the listing in the SNMP IP access list, the requester will receive a time-out error.

To authorize a management station via the SNMP IP access list:

1. Start the RLM Manager and select the Access Point RLM.
2. Click the **Edit** button to connect to the Radio Link Module.
3. Select the **SNMP** tab to display the SNMP parameters. The **SNMP IP Access List** is visible at the bottom of the **SNMP** tab as pictured in Setup SNMP parameters (page 212)
4. Use the following buttons to modify the SNMP IP access list:
   - **Add** - to add IP addresses to the list. (Press the F1 key for on-line Help for possible values for these fields).
   - **Delete** - to remove IP addresses from the list.

- **Edit** - to change entries in the list.

The default value is **<All will be permitted>**.

7.4.3 Trap Host Alerts

You can use the Trap Host mechanism to inform a network administrator when somebody resets the Radio Link Module, does the forced reload procedure or if there is an authentication failure or a link up or down is detected. The trap host alert will enable the network administrator to verify whether the reset or forced reload action was an authorized action or not.

7.4.3.1 Enable Trap Host Alerts

To activate the trap host mechanism:

1. Start the RLM Manager and select the Radio Link Module.
2. Click the **Edit** button to connect to the RLM.
3. Select the **SNMP** tab to display the SNMP parameters.
4. In the field **Trap Host IP Address** enter:
   - **Any valid IP address** - To this IP address a message is send if the Radio Link Module is reset.
   - **0.0.0.0 - (Initial value)** - To disable SNMP Trap Agent.
5. Enter a password in the field **Trap Host Password**.

   Choose a password that corresponds to the password set at the Trap Host to filter unsolicited or unauthorized SNMP Trap messages at the Trap Host.

The Trap Host IP Password will be embedded in the SNMP Trap messages sent by this RLM. If the Trap Host receives a message without or with an unknown password, the Trap message will be ignored.

- **Valid Values**: Any alphanumeric value in the range of a-z, 0-9 with a minimum of 2 and a maximum of 31 characters.
- **Initial Value**: public

6. Press **OK** to return save the new configuration to the Access Point RLM and to return to the main RLM Manager window.

When you activate the trap host alerts, be aware of the following:

- The IP address should identify the trap host station, i.e. the network management station that will be used to receive the trap messages.
- The trap host password is included in the trap messages and will help the trap host station to identify whether a received trap host message came from its own domain or not.

7.4.3.2 Trap Host Messages

The following message types can be distinguished:

- Call boot trap messages
- Authentication failure messages
- Link up or down messages

7.4.3.3 Call Boot Trap Messages

A Call boot trap message can occur in one of the following situations:

- Radio Link Module is reset

- Power down
- RLM configuration has been changed

7.4.3.4 Authentication Failure Messages

This message type is sent to the LAN administrator station once a wrong password has been entered on a (mobile) station. However, the Radio Link Module itself does not respond, a time out error occurs.

7.4.3.5 Link Up or Down Messages

This type of message can be used to signal a problem with link integrity. If, for example, in a duplicate Ethernet connection, an Ethernet link is broken, a Trap message “link down” is sent. As a result of this message, the other Ethernet connection will be used. Once the link is restored, the original connection, a “link up” message will be generated. The original connection can be used again.

7.5 Advanced Security Maintenance

7.5.1 Maintaining Access Control Tables

It is best to create a single access control table and store it on the harddisk of the LAN administrator station and/or share it with other LAN administrator stations. You are advised to use only one table for all Radio Link Modules.

For more information refer to Creating/Editing an Access Control Table (page 161).

7.5.2 Maintaining WEP Encryption Keys

The WEP Encryption functionality allows the wireless system to support up to four different keys simultaneously. This is in accordance with the 802.11 standard, which defines four so-called "default keys."

These keys can be used to smooth the transition from the usage of one key to usage of a next key. The general requirement for two cards to transmit encrypted between each other is that they share a common key value at the same key-index number in the 4-key area at the moment of transmission. The key-index of the key that was used for encryption is transmitted in clear-text in the header of the message, and will be used at the receiving side to determine which of the 4 keys to use for decryption.

It is not mandatory that both sides (typically RLM and SIMATIC NET Industrial Wireless LAN station) have the same active set of 4 keys. As long as there is one key in common, they can communicate, provided they both use that common key.

NOTE:

The 802.11 standard also defines the possibility for having a unique key per Station, tied to the station's MAC Address. SIMATIC NET Industrial Wireless LAN currently does not support that feature of the standard WEP function.

When planning the usage of different keys over time a number of aspects have to be considered:

- the length of time one key stays in use;
  this is a direct trade-off between security level (= the chance of someone finding out what the key value is) and operational overhead (= the efforts to reconfigure Access Point RLM and SIMATIC NET IWL stations)
- the requirements for smooth transition from one key to another
- the minimization of end user exposure to key values

The key roll-over possibilities built in the 802.11 standard and offered by SIMATIC NET Industrial Wireless LAN allow for a number of scenarios, each with different values for the above aspects.

The sequence of key configuration settings at Radio Link Module (shown as AP=Access Point) and SIMATIC NET IWL Station (shown as STA) over time is shown in a number of tables below. Each table reflects a certain key roll-over strategy. Notice that the column "Outward Key" shows which key is used to encrypt traffic from AP to STA and the column "Inward Key(s)" indicates the key(s) that are allowed and possibly used to encrypt traffic from STA to AP. The WEP Keys that are configured are shown in order of index number 1-2-3-4; the column "Tx" is the index number configured for

transmission. The key values are shown by capital letters to indicate a real key or by zero to indicate a non-configured index.

The column “Keys 1-2-3-4” shows an equal sign (=) when the value does not change from the previous period. This is particularly relevant when it concerns the stations keys, since it is envisaged that knowledge of the key values is typically not transferred to the end users, so they have to return their station equipment to an IT department to get the key values changed. It is envisaged that changing the Txkey Index is an action that can be done by end users, since it does not reveal secret information.

Three key roll-over strategies are distinguished:

- Single Key – No Transition (page 185),
- Single Key – Transition Period (page 187), and
- Alternative Schemes (page 188).

7.5.2.1 Single Key – No Transition

Table 4 Single Key - No Transition shows a system, where at each point in time only one single key is used. The key to be used is dictated by the AP settings, showing only one valid key at each period. This requires a change over of keys at all stations more or less synchronous with the Radio Link Module configuration changes. This is not practical and hence there are four keys.

Table 4 Single Key - No Transition

Period		AP Configuration		Out-ward Key	STA Configuration(s)		In-ward Key
#	Description	Keys 1-2-3-4	Tx		Keys 1-2-3-4	Tx	
0	Main life key A	A-0-0-0	1	A	A-B-C-D	1	A
1	Main life key B	0-B-0-0	2	B	=	2	B
2	Main life key C	0-0-C-0	3	C	=	3	C
3	Main life key D	0-0-0-D	4	D	=	4	D
4	Main life key E	E-0-0-0	1	E	E-F-G-H	1	E
5	Main life key F	0-F-0-0	2	F	=	2	F

By initially configuring all stations with the keys for the first 4 periods, only the Txkey index needs to be changed at all stations for the first three steps. At the step from period 3 to period 4, the keys have to be changed at all STAs as well.

7.5.2.2 Single Key – Transition Period

To introduce a transition period between the main life of the successive keys, the scheme has to be changed as shown in Table 5 Single Key - Transition Period.

Table 5 Single Key - Transition Period

Period		AP Configuration		Out-ward	STA Configuration(s)		In-ward
#	Description	Keys 1-2-3-4	Tx	Key	Keys 1-2-3-4	Tx	Key
0	Main life key A	A-0-0-0	1	A	A-B-C-D	1	A
1	Transition A-B	A-B-0-0	2	B	=	1|2	A | B
2	Main life key B	0-B-0-0	2	B	=	2	B
3	Transition B-C	0-B-C-0	3	C	=	2|3	B | C
4	Main life key C	0-0-C-0	3	C	=	3	C
5	Transition C-D	0-0-C-D	4	D	=	3|4	C | D
6	Main life key D	0-0-0-D	4	D	=	4	D
7	Transition D-E	E-0-0-D	1	E	A-B-C-DE-F-G-H	4 1	D E
8	Main life key E	E-0-0-0	1	E	E-F-G-H	1	E
9	Transition E-F	E-F-0-0	2	F	=	1|2	E | F

Notice that in the transition periods 1, 3 and 5 the end users can switch over from one Txkey index to the next. At the end of this period, all stations must be over to the new key index. Transition period 7 includes the transition to a new set of keys as well. The total length of time a key is used consists here of the main life time period and two transition periods. Assuming the main

life is much bigger than the transition, this can still be considered to be a single key scheme, because most of the time only a single key is in use.

7.5.2.3 Alternative Schemes

Alternative schemes can be envisaged, which have main life periods in which two or more keys are active. An example is given in Table 6 Alternative Schemes

Table 6 Alternative Schemes

Period		AP Configuration		Out-ward	STA Configuration(s)		In-ward
#	Description	Keys 1-2-3-4	Tx	Key	Keys 1-2-3-4	Tx	Key
0	Main life key A	A-0-0-0	1	A	A-B-C-D	1	A
1	Main life A+B	A-B-0-0	2	B	=	1|2	A | B
2	Main life B+C	0-B-C-0	3	C	=	2|3	B | C
3	Main life C+D	0-0-C-D	4	D	=	3|4	C | D
4	Main life D+E	E-0-0-D	1	E	A-B-C-D E-F-G-H	4 1	D E
5	Main life E+F	E-F-0-0	2	F	E-F-G-H	1|2	E | F

Table 6 Alternative Schemes gives a scheme where at each period two keys are in use; at the end of each period, the oldest key is no longer valid and needs to be replaced at all stations. Advantage of this scheme versus the scheme in Table 5 Single Key - Transition Period is that it requires less frequent configuration changes at all Radio Link Modules.

8 Advanced Network Configurations

8.1 Introduction

To configure your SIMATIC NET IWL network beyond the basic configuration a number of advanced aspect will be discussed:

- Advanced Parameters (page 191),
- Configuring Large Networks (page 218),
- Modifying the Configuration (page 226),
- Restoring a Back-up Configuration (page 228),
- Dual PC Card Configuration (page 229),
- About IP Addresses and Subnets (page 229).

8.2 Advanced Parameters

You may wish to explore the "Advanced Parameters" options as supported by your Radio Link Modules, especially when administering larger networks that encompass more than 10 RLMs.

Advanced parameter options include:

- Advanced parameters, such as, RTS/CTS Medium Reservation, Distance between Access Point RLMs.
- Bridge parameters that enable you to filter specific networking protocols and/or traffic between specific stations.
- Access Point RLM parameters, or
- SNMP parameters

For most networks, the default settings for the advanced parameters will provide more than reliable network connectivity. You are advised to change these parameters only when you are familiar to the type of parameters, for example based upon your experience and expertise with similar parameters in wired and/or SIMATIC NET IWL networking environments.

NOTE:

A number of the advanced parameters described below may be marked as "common" parameters. This means that they should be the same for all Radio Link Modules in your network (see also Configuring Large Networks (page 218)).

To set the advanced parameters, simply follow the instructions as described in the previous section, Configuring Infrastructure Networks (page 58), to connect to the Access Point RLM that you wish to configure.

8.2.1 Advanced Parameters

If you created a basic Access Point RLM configuration, as described in the previous section, you may have already noticed the additional buttons in the setup window, as pictured in RLM Manager Wireless Interfaces tab (page 64).

8.2.1.1 Frequency

The Frequency setup menu gives you the ability to select an operating frequency from a range of sub-channels within the 2.4 GHz frequency band. The number of selectable channels is determined by the radio regulations that apply in your country.

Click the **Advanced** button on the **Wireless Interfaces** tab of the edit mode to change the frequency parameters.

To optimize network traffic, we recommend that you assign different operating frequencies to Radio Link Modules that service neighboring wireless cells. Doing so, stations in each of the cells will be able to use the maximum bandwidth available to their cell.

Wireless stations equipped with PC cards CP 1515 can dynamically change the operating channel when roaming between Access Point RLMs that operate at different sub-channels.

8.2.1.2 RTS/CTS Medium Reservation

RTS/CTS medium reservation may provide a solution for networks where:

- Density of stations and Access Point RLMs is very low.
- You witness poor network performance due to excessive frame collisions at the Radio Link Modules.

However in most networking environments it is very unlikely that you will need to enable RTS/CTS medium reservation on the Access Point RLM to prevent collisions. You are advised to read the information about Optimizing Wired Connections (page 121) prior to changing this setting for the Access Point RLM.

To enable RTS/CTS medium reservation click the **Advanced** button on the **Wireless Interfaces** tab.

8.2.1.3 Interference Robustness

The Interference Robustness can be activated in exceptional cases when troubleshooting slow performance of your network that could be related to in-band interference from e.g. microwave ovens. Interference will usually show a poor Signal to Noise Ratio (SNR) that is based upon a good signal level and a high noise level. This behavior is often perceived when:

- the “trouble” station or Radio Link Module is close to a interference source, or
- an interference source is located in the signal path between the “trouble” stations and the Access Point RLM.

To enable Interference Robustness click the **Advanced** button on the **Wireless Interfaces** tab in the edit mode to display the Advanced Setup window, then select the option **Interference Robustness**.

8.2.1.4 Distance Between APs

In networking environments where you have either data intensive users, or a large number of users in a small area, you may wish to consider increasing the number of Access Point RLMs (making the distance between Radio Link Modules smaller), and then adjusting the Distance Between APs parameter to optimize the load balance of the number of wireless stations per Access Point RLM.

To change the Distance Between APs parameter display the **Wireless Interfaces** tab in the edit mode and click the **Advanced** button. In the field **Distance Between APs** choose one of the three density options:

- Large - (default)
- Medium
- Small

The default setting **Large** provides a maximum wireless coverage with a minimum number of Access Point RLMs. This option which is typically used for single-cell networks, but will also provide an efficient and cost effective solution for most networks that include multiple wireless cells.

CAUTION:

The setting for distance between Radio Link Modules must be the same for all SIMATIC NET IWL equipped devices in your wireless network. A mismatch in the configuration setting for this parameter may have unpredictable performance results for wireless (mobile) stations in your network.

Medium distance between Access Point RLMs can be selected for environments where stations experience slow network response times even though the quality of radio communications is rated as excellent. The slow response times might be experienced in areas where:

- A high number of wireless stations is located close to one another, causing other stations to defer data transmissions.
- A number of wireless stations engaged in heavy network traffic is causing other stations to defer data transmissions.
- The setting **Large** creates overlapping radio cells, which may cause stations in one cell to defer data transmission for stations located in the neighboring cell.

You should only select **Small** distance between Radio Link Modules when you are designing a wireless infrastructure that will include a high concentration of Access Point RLMs: i.e. the total cost of hardware investments is less critical than the maximum data throughput per cell.

NOTE:

The settings **Medium** or **Small** distance between Access Point RLMs require a excellent quality of radio communications throughout the entire wireless coverage area. In environments where the actual placement of Radio Link Modules was designed to obtain maximum wireless coverage with a minimum number of Access Point RLMs, changing the distance between RLMs from **Large** to **Medium** or **Small** will not yield better results. Adversely, doing so might seriously affect the roaming performance of your wireless stations, risking network communication errors caused by "out-of-range" situations.

If you consider using the option **Medium** or **Small** distance between Radio Link Modules to create a high performance network, you are advised to read the section Frequency Channel Management (page 138) as well.

For more information about Access Point RLM density, please consult Optimizing Performance (page 116).

8.2.1.5 Multicast Rate

The Multicast Rate identifies the preferred transmission speed for your Access Point RLM broadcast traffic as forwarded by the Radio Link Module. Where transmissions at lower data rates are usually more reliable, you may prefer higher throughput performance over greater coverage for your wireless radio signal.

For more information about multicast rate refer to the help-file of the RLM Manager program.

8.2.2 Bridge Parameters

One of the ways to optimize the performance of your wireless networks is to prevent "redundant" traffic from being transmitted over the wireless network. Redundant traffic may include:

- Specific network protocols exchanged by networking devices such as servers, that are not relevant to the wireless stations.
- Broadcast and/or multicast messages exchanged by specific networking devices such as servers that are not specifically addressed to the wireless stations.
- "Junk traffic" like for example error messages that are generated by malfunctioning devices, or as the result of incorrect network configurations that could have been avoided (for example closed network loops).

Filtering redundant traffic will save the bandwidth of the wireless medium for the wireless stations, optimizing throughput efficiency for these stations.

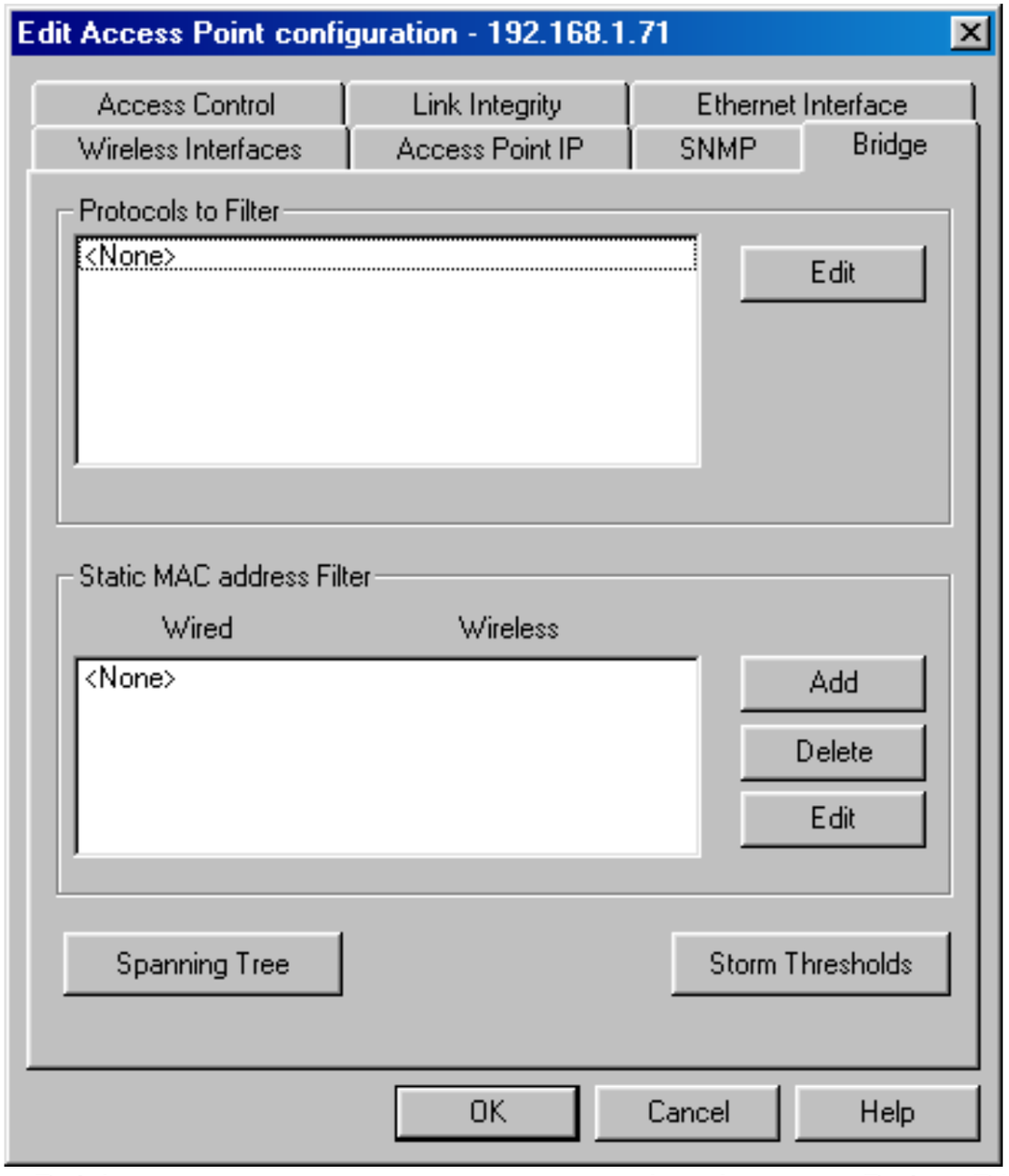
Optimizing wireless performance via the **Bridge** tab can be achieved in the following ways:

- Protocol filtering to deny specific networking protocols from being bridged to the wireless network interface (see Protocol Filtering (page 200)).
- Filtering traffic exchanged between two specific stations that are identified by their static MAC address (see Static MAC Address Filter (page 202)).
- Enabling the spanning tree mechanism to resolve the closed network loops errors (see Spanning Tree (page 203)).

- Storm threshold filtering to limit the number of messages per port and/ or station from being bridged (see Storm Threshold (page 205)).

CAUTION:
The Bridge parameter settings are typical “common” parameters, i.e. the Bridge parameter settings should be the same for all Access Point RLMs.

Figure 36 Bridge Tab in the Edit Mode



To set the Bridge parameters, connect to the Access Point RLM and select the **Bridge** tab to display the bridge parameters as pictured in Figure 36 Bridge Tab in the Edit Mode.

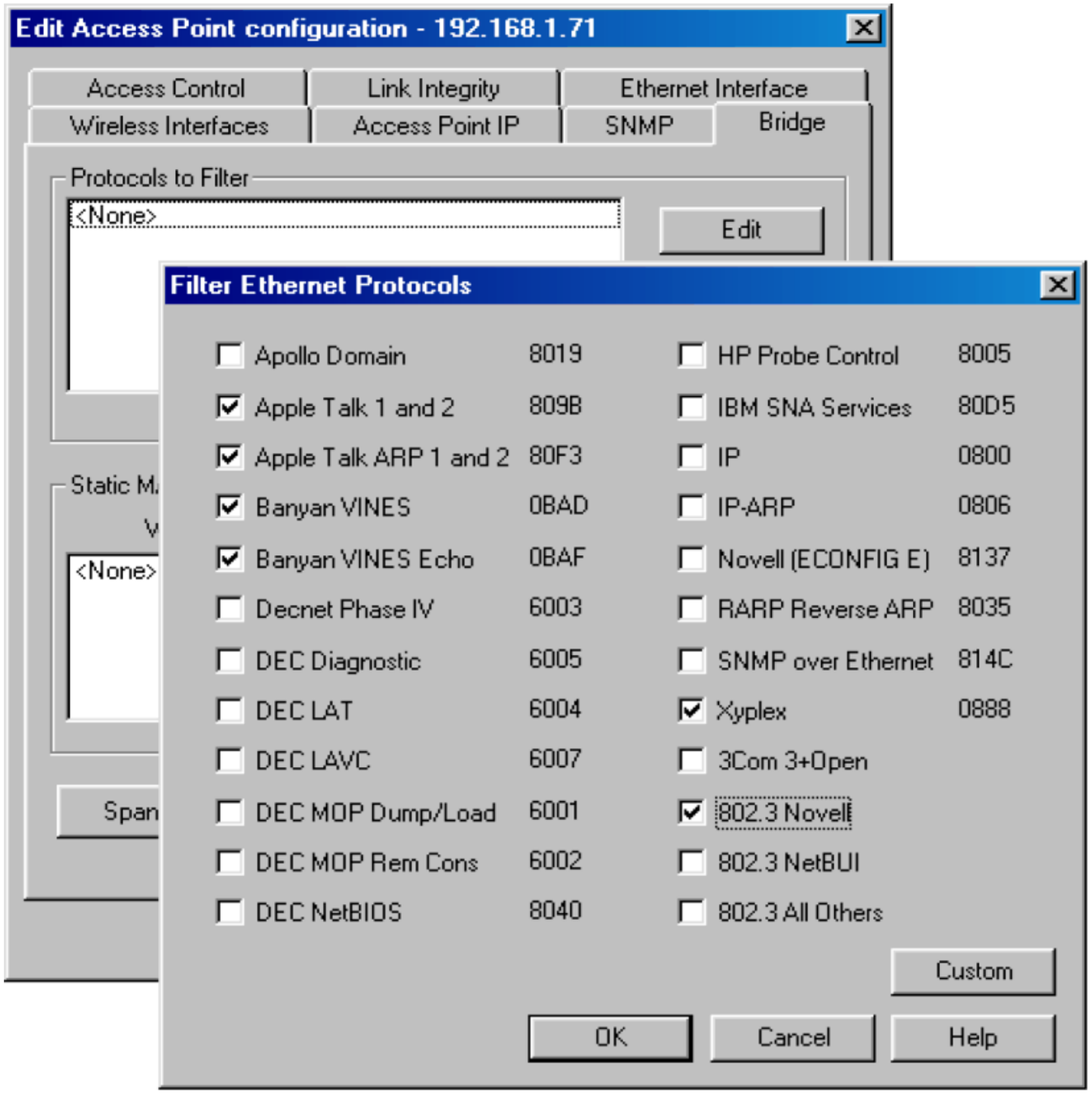
8.2.2.1 Protocol Filtering

The filtered protocols are listed in the top section of the **Bridge** tab. The factory-set default of the Radio Link Module is **<None>** which will allow all protocols to be transmitted to the wireless medium. This is the recommended setting when you do not require specific protocols to be filtered.

To filter specific protocols, proceed as follows:

1. Determine the minimum set of protocols that must be bridged.
2. Click the **Edit** button to display the Filter Ethernet Protocols window pictured in Figure 37 Select Ethernet Protocols to be Filtered.

Figure 37 Select Ethernet Protocols to be Filtered



3. Place a check mark in the check box of each protocol that does not need to be transmitted to the wireless medium.

   To stop filtering a specific protocol, clear the check box.

4. (Optional) To add a non-listed protocol to the list, click the **Custom** button to enter the protocol manually.
5. When finished click **OK** to return to the **Bridge** tab as pictured in Figure 36.

   All of the protocols that you have selected, and/or all of the custom protocols that you have added manually, will be listed in the **Protocols to Filter** field.
6. You can now select one of the other Bridge parameter options, change other parameters or click **OK** to save your changes and return to the main RLM Manager window.

8.2.2.2 Static MAC Address Filter

To filter out traffic exchanged between stations that is not required to be sent or received via the wireless interface, you can set the **Static MAC address Filter** in the bottom section of the **Bridge** tab. The default value, **<None>** will be acceptable for most networking environments (see Figure 36 Bridge Tab in the Edit Mode).

You can use the MAC filtering option for example to filter broadcast or multicast messages exchanged between wired servers that can receive each others messages also via the wired network.

To filter out traffic between such devices add the MAC addresses of both devices as a pair in the **Static MAC address Filter** list.

The way the filter works is that when one of the listed stations sends a message to a MAC address that has been identified as a pair, the Access Point RLM will not forward it via the wireless station. All traffic that one of

the stations wishes to send to any other (non-paired) MAC address will be forwarded.

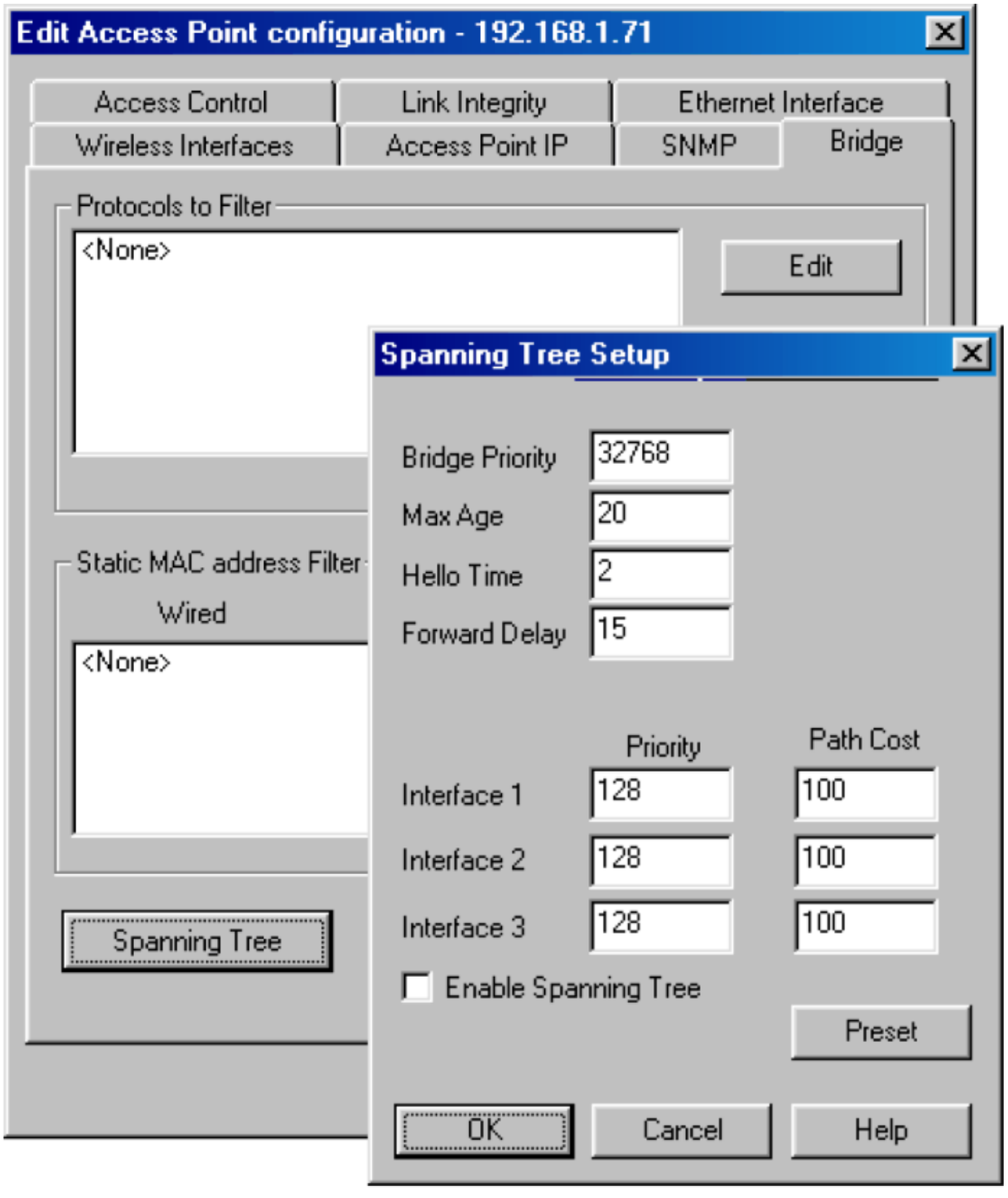
For more information about static MAC address filtering, please refer to Optimizing Performance (page 116).

8.2.2.3 Spanning Tree

The **Spanning Tree** button allows you to set parameters that are used in determining the optimum path for network traffic to travel.

You can use spanning tree in a network that has been designed to include loops, such as a redundant wired link used as a back-up to the main wireless link.

Figure 38 Spanning Tree Setup window



To enable spanning tree:

1. Click the **Spanning Tree** button to open the Spanning Tree Setup window (see Figure 38 Spanning Tree Setup window).
2. Click the **Enable Spanning Tree** check box;
3. Use default values (see Figure 38 Spanning Tree Setup window);
4. Click **OK** to return to the **Bridge** tab.
5. Click **OK** again if you want to save this configuration and return to the main RLM Manager window. Otherwise continue changing other parameters.

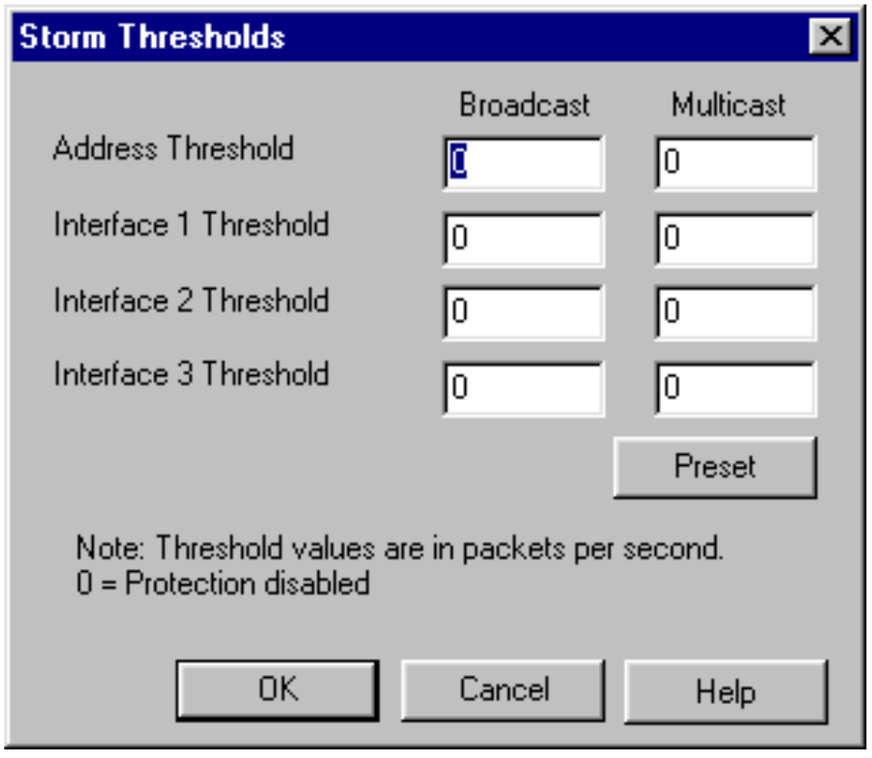
At this point, we recommend that you create a backup file, as described in Step 4 - Create a Back-up of the Configuration (page 66).

8.2.2.4 Storm Threshold

The **Storm Thresholds** button allows you to set parameters that are used in protecting the network against message overload as received from a single station or via a specific port.

The **Storm Thresholds** window allows you to determine the maximum number of multicast and broadcast messages that will be forwarded from one port (or address) per second.

Figure 39 Storm Thresholds Protection Disabled



The factory-set configuration for storm threshold protection is disabled (all values are set to zero).

1. If you need storm threshold protection, and are unsure of the proper broadcast and multicast values to input, click the **Preset** button for values that will provide adequate levels for most networking environments.
2. Click **OK** to keep these settings and return to the **Bridge** tab.

Click **OK** again if you want to save this configuration and return to the main RLM Manager window. Otherwise continue changing other parameters.

8.2.3 Access point IP Parameters

The Access Point IP tab enables you to set the common IP parameters and to change the unique IP address of your Radio Link Modules.

To change the IP parameters proceed as follows:

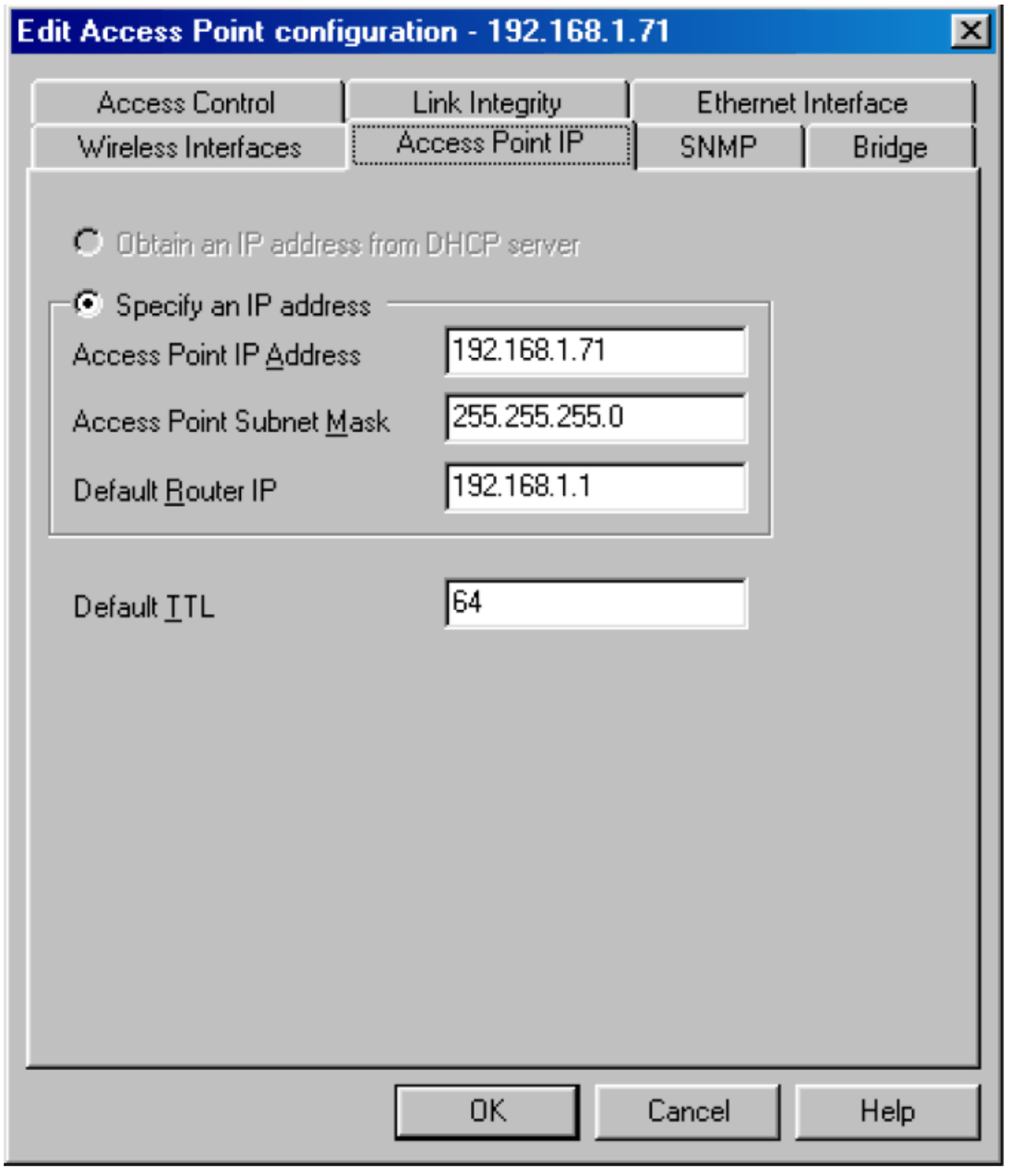
1. Make sure you are connected to the right Access Point RLM in the edit mode and select the **Access Point IP** tab to display the IP parameters (see Figure 40 Setup Radio Link Module IP Parameters).
2. Verify and/or modify the parameters of your choice.

   The mandatory parameters that you must specify are:

   - **Acess Point IP** address (unique for each Access Point RLM, in case of a BOOTP or DHCP server, this IP address is entered automatically).
   - Access Point **Subnet Mask** (the same for all Radio Link Modules, in case of a BOOTP or DHCP server, this IP address is entered automatically).
   - (optional) **Default router** (usually the same for all Access Point RLMs.
   - (optional) **Default TTL** (Time To Live) (usually the same for all Access Point RLMs).

   All parameters are explained in the next paragraphs.
3. When finished, proceed with configuring other parameters or click **OK** to save the configuration and return to the main RLM Manager window.

Figure 40 Setup Radio Link Module IP Parameters



8.2.3.1 IP address

Each Access Point RLM needs an unique IP address. Use either:

- DHCP, to obtain an IP address automatically, or
- manually enter an IP address

NOTE:

All Access Point RLMs must have a unique IP address value to allow you to address each Radio Link Module specifically. Duplicate IP address values may cause unexpected behavior of the network and/or negative impact on network performance.

8.2.3.1.1 Manually assign an IP address

In case of manually assigning an IP address, use the field **Access Point IP Address** to enter a value from the range of IP addresses assigned to your organization.

The IP address is primarily used to address this Access Point RLM when you use the RLM Manager program to configure and/or monitor this device.

When your organization does not use IP addressing, you can enter a user-defined value. For example a value of the same pattern as the factory-set IP address 153.69.254.254, where you replace the last three digits with a numerical value in the range of “1” to “253.”

8.2.3.1.2 Automatically assign an IP address

In case when a DHCP server is available on the network, an IP address will be automatically assigned to the Radio Link Module by the DHCP server. To enable automatically obtaining an IP address form the DHCP server, select

the field **Obtain an IP address from DHCP server** on the **Access Point IP** tab.

For more information about DHCP refer to BOOTP and DHCP (page 231).

8.2.3.2 Subnet Mask

The field **Access Point Subnet Mask** is a common parameter and must be the same for ALL network devices within your IP subnet.

You can use either the default value (255.255.0.0) or change the subnet mask to a value that applies in your network.

If **Obtain an IP address from DHCP server** is enabled, the subnet is also automatically entered.

8.2.3.3 Default Router

The field **Default Router IP** is an optional field that is relevant when you intend to use the Radio Link Module support for TRAP messages (see also SNMP Parameters (page 211)).

You can use the Default Router IP field to identify the IP address of the router which the RLM will use to find the Trap Host IP Address (identified in the SNMP Parameters).

The default router and the trap host IP address described later in this chapter are only used for TRAP messages generated by the Access Point RLM upon a reset, modification of the configuration, or forced reload procedure.

If the value of the field **Default Router IP** is set to 0.0.0.0 (default), then no TRAP messages are initiated by this Radio Link Module.

The Default Router is also relevant if you want to manage (or just ping) the Access Point RLM from an other subnet.

8.2.3.4 Time To Live (TTL)

The field **Default TTL** (Time To Live) identifies the maximum number of hops for an IP message generated by the Access Point RLM (typically used for the trap host messages).

The value will be decreased each time the message passes a router. When the TTL value becomes 0, the message will be rejected by the next router it meets. By default, the value is 64.

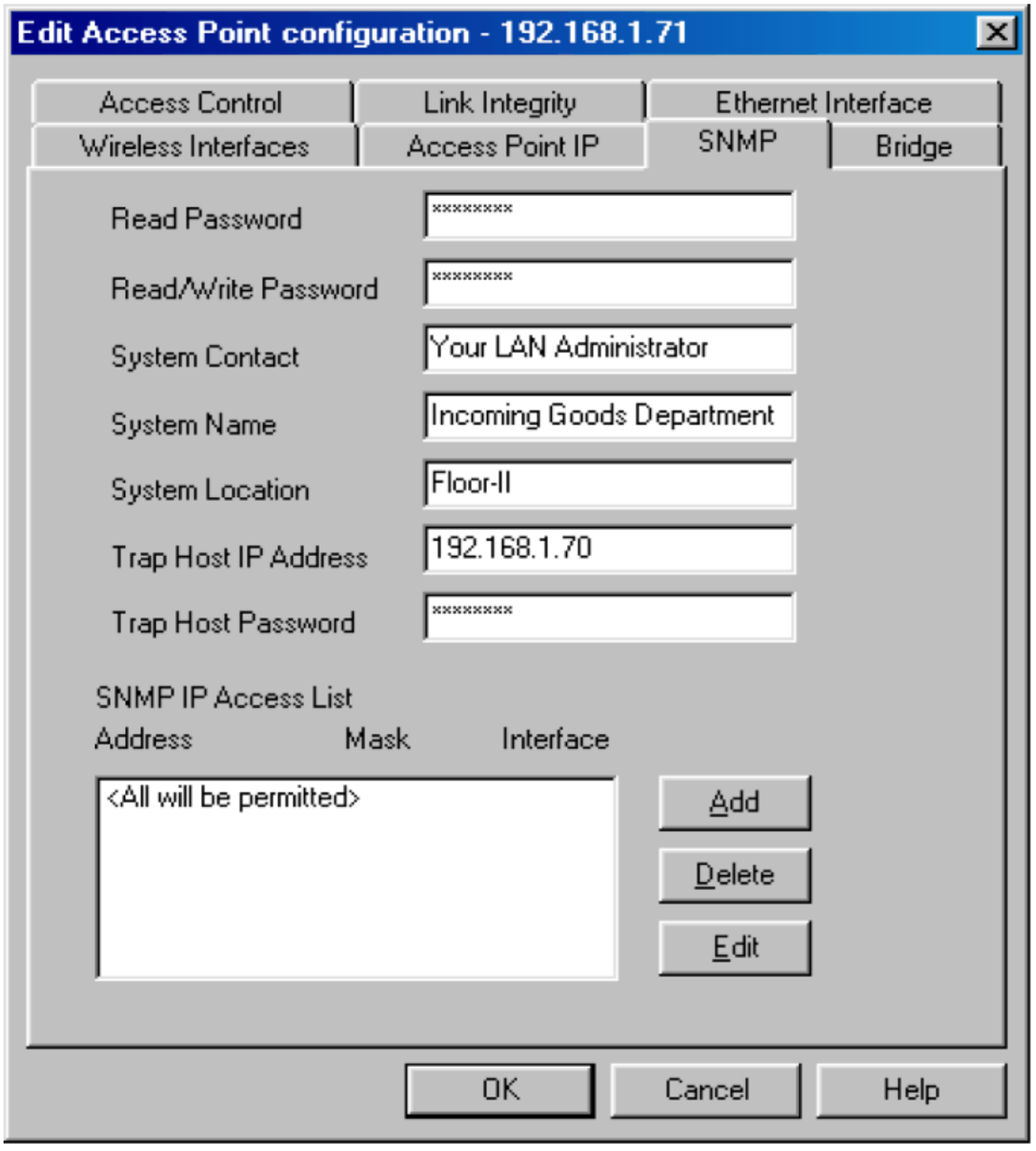
8.2.4 SNMP Parameters

Most SNMP parameters (except for the System Location and System Name) are common parameters, i.e. they should be the same for ALL Radio Link Modules in your network.

To set the SNMP parameters proceed as follows:

1. Make sure you are connected to the right Access Point RLM and select the **SNMP** tab to display the SNMP parameters pictured in Figure 41 Setup SNMP parameters.

Figure 41 Setup SNMP parameters



2. Verify and/or modify the parameters of your choice.

   The recommended parameters that you should specify are:

   - **Read/Write Password** to restrict access to the configuration of your Access Point RLMs, and

- **System Name** to allow easy identification of the Radio Link Module when using the diagnostic options of your software tools.

These and all other SNMP parameters are explained in the following paragraphs.

3. When finished, proceed with configuring other parameters or click **OK** to save the configuration and return to the main RLM Manager window.

8.2.4.1 Read Password

Change the **Read Password** parameter in order to prevent unauthorized access to the Access Point RLMs.

A read password is requested when you connect to RLMs with the **Monitor** option. The default value is "public."

With the correct read password, a local LAN administrator can only monitor Radio Link Module statistics and tables, but not view or change any of the parameters.

8.2.4.2 Read/Write Password

Change the **Read/Write Password** parameter in order to prevent unauthorized access to the RLMs to make changes to its configuration settings.

A read/write password is requested when using the **Edit** button to connect to the Access Point RLM. The default value is "public."

With the correct read/write password, a network supervisor can monitor Radio Link Module statistics and view or change any of the parameters of the configuration. Using different values for the Read and Read/Write

Password parameters you can create different levels of authority for your LAN Administrators to configure and/or monitor the RLMs.

8.2.4.3 System Contact

Use the field **System Contact** to enter a generic name for the network supervisor or department, (e.g. “Your LAN Administrator” as pictured in Figure 41 Setup SNMP parameters).

8.2.4.4 System Name

Use the field **System Name** field to enter a generic logical location of the Access Point RLM, (e.g. “Incoming Goods Department” as in Figure 41 Setup SNMP parameters).

8.2.4.5 System Location

Use the field **System Location** to enter a generic physical location of the Radio Link Module, (e.g. Access Point RLM floor 1N as in Figure 41 Setup SNMP parameters).

8.2.4.6 Trap Host IP Address

If you plan to use the trap alert system as described on Trap Host Alerts (page 180), you can use the **Trap Host IP Address** field to enter the address of the network management station that should collect the SNMP trap messages. If you do not intend to use trap host alerts, the value is set to “Don’t care.”

For more detailed information about trap host messages, see Trap Host Alerts (page 180).

8.2.4.7 Trap Host Password

Use the **Trap Host Password** field to enter a password that will be included in the SNMP trap messages. You can use this password at the trap host station to filter out trap messages that may have been sent to the trap host station erroneously.

8.2.4.8 SNMP IP Access List

You can use the **SNMP IP Access List** to create an extra level of security in addition to the read an read/write passwords. This will allow you to authorize a limited number of LAN administrator stations to view and/or modify the configuration of the RLMs, based upon the IP address of these stations.

The field **SNMP IP Access List** should typically include the IP address of all LAN administrator stations that will use the RLM Manager to configure and/or monitor your Radio Link Modules.

To authorize the LAN administrator station you must enter:

- The IP address of the station(s), and
- The Access Point RLM network interface through which they will access the Access Point RLM.

To indicate the interface, use either:

- “1” for Ethernet
- “2” for the wireless network interface in socket A, or
- “3” for the wireless network interface in socket B.

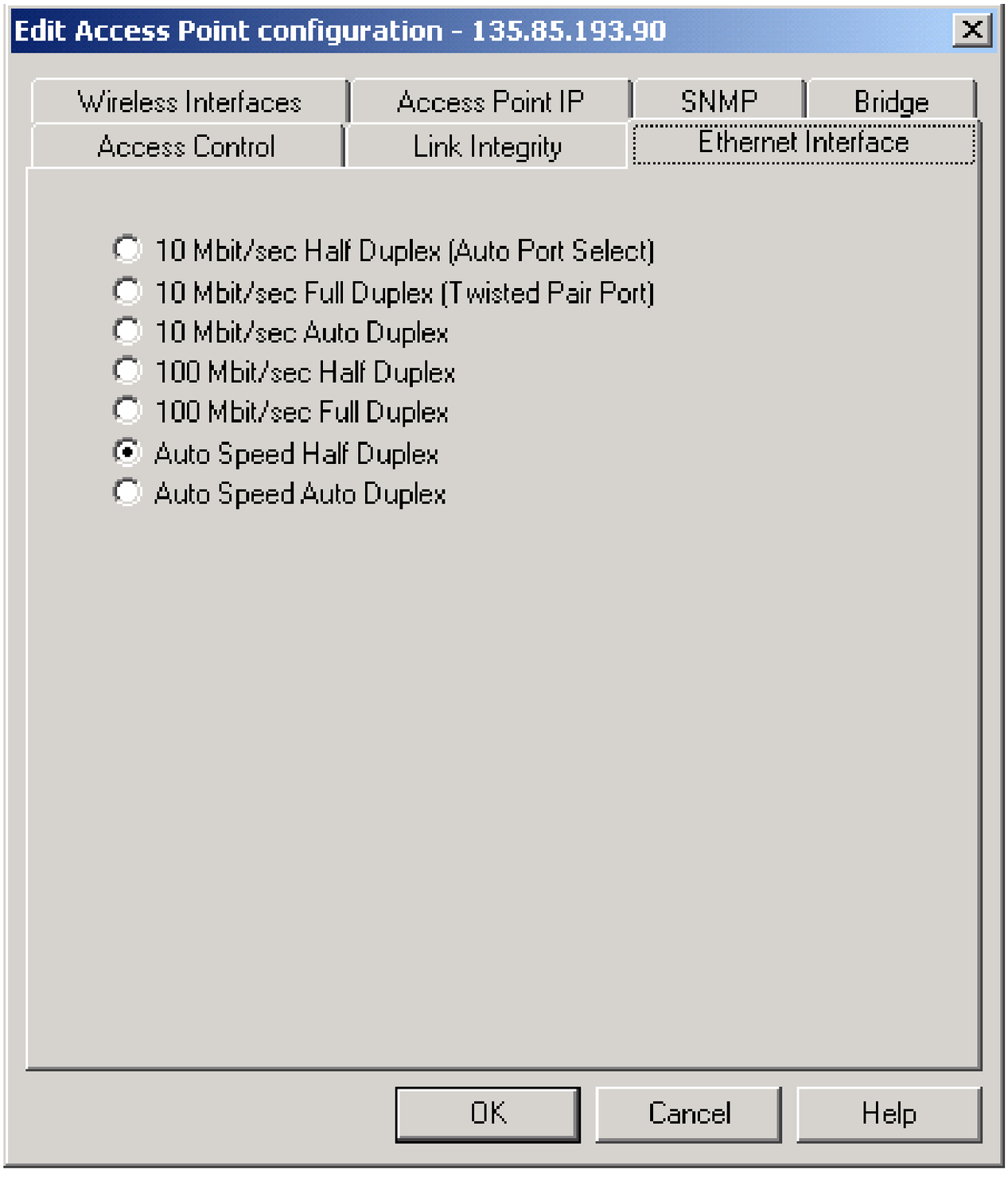
Alternatively you can use the value “x” to allow the identified IP address to access the Radio Link Module via any of the available interfaces.

To allow multiple LAN administrator stations to access the RLM configuration and/or monitor parameters, you can also assign a range of IP addresses. Doing so, enter a subnet mask value that will indicate the subnet from which all stations are authorized to modify the SNMP setup.

8.2.5 Ethernet Interface

Subject to the type of interface offered by your Access Point RLM, you can select one of the options (see Figure 42 Select Ethernet Interface).

Figure 42 Select Ethernet Interface



For more information about selecting the Ethernet Interface refer to the help-file of the RLM Manager program.

8.3 Configuring Large Networks

Each Radio Link Module configuration is characterized by two types of parameters:

- Common parameters that must be the same for ALL RLMs in your network, and
- Unique parameters that must be unique for each Access Point RLM in your network.

In larger networking organizations, it may become quite cumbersome to copy the common parameters to each of the Radio Link Modules in the network in order to provide consistency throughout the entire network. As the number of RLMs increases, the risk of errors (e.g. as a result of typos) may increase as well.

Inconsistent values for common parameters, or duplicate values for the unique parameters may have unpredictable effects on the performance of your network. Document the configuration settings of your network in detail to avoid configuration mismatches.

Therefore, we recommend that you create a template file that contains all of the common parameter settings that apply to every Access Point RLM within the network.

8.3.1 Common Parameters

Common parameters, such as the network name or SNMP Read/Write Password, are used to identify which Radio Link Modules belong to the same network environment. They differentiate your group of RLMs from other (neighboring) network environments.

A list of common parameters is shown in Table 7 Common RLM Parameters below, together with the RLM Manager tabs where you can view or modify the parameters.

Table 7 Common RLM Parameters

Parameter	RLM Manager tab
• Network Name	Wireless Interfaces
• Protocols to Filter • MAC Filtering	Bridge
• Radio Link Module Subnet Mask • Default Router IP • Default TTL	Access Point IP
• Read Password • Read/Write Password • SNMP IP Access List • (optional) Trap Host IP Address and Password	SNMP

8.3.2 Unique Parameters

Unique parameters such as the IP Address or System Name, are used to differentiate a single Radio Link Module from the group of RLMs that are operated within your network. The most important unique parameters are listed in Table 8 Unique RLM Parameters.

Table 8 Unique RLM Parameters

Parameter	RLM Manager Setup Menu
• Radio Link Module IP Address	Access Point IP
• System Name • System Location	SNMP

8.3.3 Managing Configuration Consistency

The most convenient way to manage the configuration of a large number of Radio Link Modules is to configure the first Access Point RLM and save its configuration to file. Use this file as a template that you can upload to the other RLMs.

After loading the template file on each Radio Link Module, you will modify the parameters identified as the unique parameters, to differentiate the RLM from the other Radio Link Modules in this network.

In other words, the easiest way to manage a large number of RLMs is as follows: Access Points (RLMs

1. Preparation
   Identify and record all information related to each of the Radio Link Modules to be configured.
2. Creating a template file
   Identify and set the common parameters that should apply to all RLMs within your network.
3. Configuring all Radio Link Modules
   Import the template file and modify all the unique identifiers to differentiate the Access Point RLM from the other RLMs.

CAUTION:
We recommend that you create a backup file for each unique Radio Link Module configuration, using the Download Config File item from the RLM menu in the main RLM Manager window. Use a file name that allows you to easily recognize the relationship between a file name and the specific RLM.

8.3.3.1 Preparing Large-Scale Networks

To prepare the configuration, you need to carry out the following activities:

- Unpack the RLM and record their serial number and MAC address on the “Access Point Configuration Record” as printed in Start-up Configuration (page 232) of this document.
- Make a list of IP addresses available in your network, you will need one IP address for each Radio Link Module.

- Use the “Access Point Configuration Record” to assign one IP address to each of your RLMs.
- Record the intended system location of each Radio Link Module on the “Access Point Configuration Record”.

8.3.3.2 Creating a Template File

1. To create a template file, configure the first Access Point RLM as described earlier under Configuring Infrastructure Networks (page 58).
2. Save the configuration of this Radio Link Module to disk as described in Step 4 - Create a Back-up of the Configuration (page 66).
3. Create a copy of the back-up file with the name “common.cnf” or any other name that will allow you to easily recognize the file as the actual template file that we will use as the basis to configure the other RLMs in your network.

CAUTION:

Do not start using your original back-up file as template file. Any changes you make to the file might impair your ability to fully restore the original configuration of your first RLM, if the unit goes out of service. Always store back-up copies on a separate disk and/or location.

8.3.3.3 Configuring other Radio Link Modules

Having created the template file, we can now start (re-)configuring the other RLMs in batch-mode. For each Access Point RLM, the procedure will be as follows:

- Run RLM Manager and connect to the target Radio Link Module.
- Upload the template file that contains the values that are common for all RLMs from a template file.
- Set the unique parameters for each Access Point RLM.
- Save the values to an individual configuration file on disk.

The detailed procedure is as follows:

1. Start the RLM Manager program.
2. Select the target Radio Link Module from the list or enter a specific Access Point RLM IP address. If the target Access Point RLM is not displayed in the list, choose **Refresh** Radio Link Module **List** from the RLM menu.

   If the selected Access Point RLM is still using the factory-set IP address, for example when you are configuring a new “out-of-the-box” Radio Link Module, you will be prompted to change the default IP address as described earlier in Step 2 - Connecting to the Access Point RLM (page 60).
3. When asked navigate to the disk and/or folder where you stored the template file.
4. Select the template configuration file (e.g. **“**common.cnf”) and click the **Open** button.

WARNING:
The IP address that was displayed in the list in the main RLM Manager window has been overwritten with the IP address which was specified in the template file. Follow the

procedures described below to change it to the desired IP address value. Failing to do so may lead to multiple RLMs being configured with the same IP address, resulting in unpredictable network behavior.

The RLM Manager program has now loaded the settings as identified in the template file. Now you must change all the parameters that should be unique to this Access Point RLM (see Unique Parameters (page 220)) prior to saving the configuration and returning to the main Radio Link Module window by clicking **OK**.

5. Set the unique parameters that apply to this Access Point RLM.

   The minimum set of unique parameters that you must set are listed in Table 8 Unique RLM Parameters.

6. Now save the configuration to the Access Point RLM, by clicking the **OK** button. You return to the main Radio Link Module window.

7. Create a back-up file of the configuration for this Access Point RLM, using the **Download Config File** command from the RLM menu.

   Use a file name that allows you to easily recognize the relationship between the file name and this Radio Link Module.

The entire set of common and unique parameters are now saved permanently into the (non-volatile) FlashROM of the Access Point RLM. They will remain stored in the RLM, even if the Radio Link Module is reset or switched off and on again.

Repeat step 2 - 7 for every other Access Point RLM that you wish to configure.

8.3.3.4 Completing the Installation

When you configured the RLMs at your desk, i.e. the Radio Link Modules were not yet installed into their intended location, label each Access Point RLM with clear instructions for your installation technicians.

1. Record the intended location of the Access Point RLM on a label and attach the label to the Radio Link Module.
2. Record the name of the file with the RLM's configuration data and the location where you will install the Access Point RLM on the "Access Point Configuration Record."
3. When finished, store the back-up files (*.cnf), your template file (**"**common.cnf") and your "Access Point Configuration Record" in a safe place.

8.4 Modifying the Configuration

You can modify the Access Point RLM configuration parameters using the **Edit** button from the main RLM Manager window.

Keep in mind that you will need to address the Radio Link Module using its new IP address and the new read/write password (if you changed the Read/Write Password parameter) to open the configuration file. If your SIMATIC NET IWL management station is a wireless station, you may need to modify the station's interface parameters to match the values that were originally stored in the Access Point RLM.

Alternatively, if you have forgotten the read/write password, or any other setting required to access the RLM, you may need to do a forced reload, as described in Forced Reload Procedure (page 244).

NOTE:

When you make changes to the configuration of a particular Radio Link Module, you should update the "Access Point Configuration Record" to reflect these changes.

8.4.1 Changing Common Parameters

If you need to make changes to the common parameters, i.e. the parameters that apply to all Radio Link Modules, the most efficient way to do so is as follows:

1. Change the common parameters for one Access Point RLM.
2. Save the changes to a new template file (e.g. “common.cnf”)
3. Follow the procedure as described in Configuring other Radio Link Modules (page 222).

8.5 Restoring a Back-up Configuration

To restore previously saved back-up configuration files to your Access Point RLM proceed as follows:

1. Start the RLM Manager program.
2. Select the Radio Link Module you want to upload the configuration file to.
3. From the Access Point RLM menu select **Upload Config File**.
4. Select the configuration file you want to upload, and click **Open**.
5. When prompted to confirm the upload, verify whether the pop-up message reflects the correct IP address.
   - When the IP address value is correct, click **Yes** to proceed. The Access Point RLM will now reset automatically.
   - If the IP address is not correct, click **No** to return to cancel the upload procedure

The new parameter settings will now be loaded into the FlashROM of the Radio Link Module. This means that the parameters will remain intact whenever the RLM is reset or switched off and on again. To change the parameters again, simply repeat the procedure as described in this section to reconfigure your RLMs.

8.6 Dual PC Card Configuration

The use of two PC Cards CP 1515 in one RLM can serve multiple purposes, e.g.:

- Doubling the capacity of the Radio Link Module.

A second PC Card inserted in the second slot of the Access Point RLM will double the capacity of the Access Point RLM. This option might be used in cases where a high rate of lost messages prevent fast data communication.

8.7 About IP Addresses and Subnets

In larger organizations that make use of IP addressing for communications, the network architecture may include different network segments (subnets), typically separated by a router or gateway.

When installing the SIMATIC NET IWL infrastructure into this type of network architecture, please note that all Radio Link Modules and wireless stations must be installed on the same subnet, i.e. on the same side of the router or gateway.

The roaming functionality does not work over routers. When RLMs are connected to different subnets, a mobile station may lose its network connection when it physically enters an area where the RLMs are connected to a different subnet.

The configuration and management of your Radio Link Modules is managed via the TCP/IP protocol stack. This means that each Access Point RLM and computer that you wish to use to configure the RLMs must have a unique IP address.

You are advised to assign “static” IP addresses to the Radio Link Modules as described earlier in this chapter. This ensures that the RLMs at specific locations will always have the same IP address. For the LAN administrator stations you may either use a “static” IP address or a dynamic IP address that is assigned by a BOOTP or DHCP server.

When assigning IP addresses to LAN administrator stations and RLMs, make sure that:

- Each device has a unique IP address.
- All devices use the same subnet mask.

NOTE:

The wireless networking system does not need IP addressing to connect normal wireless stations to the network. The infrastructure is just the “physical” medium to connect a computer to an Radio Link Module, like you could use wire to connect it to an Ethernet infrastructure.

However in environments where the network operating system uses the TCP/IP protocol, stations may need to have an IP address as well to use specific networking services, like for example access to the internet.

8.7.1 BOOTP and DHCP

When powered-up for the very first time, the Access Point RLM will broadcast a request for an IP address. If your network includes a BOOTP or DHCP server, this server will automatically assign an available IP address to the Access Point RLM.

Subject to the settings of your BOOTP or DHCP services, you may need to introduce the Radio Link Module MAC address to the BOOTP or DHCP server. Consult the documentation of your BOOTP/DHCP software for more information.

An IP address that is assigned by a DHCP server will be stored in the volatile memory of the Access Point RLM: i.e. if the RLM is reset, the DHCP server may assign another IP address. To obtain consistency in the IP address, it is advised to assign a permanent IP address to the Radio Link Module, using the **Access Point IP Address** field on the **Access Point IP** tab.

An IP address that is assigned by a BOOTP server is stored in the configuration file of the BOOTP server. This configuration file has a one-to-one (static/fixed) mapping from MAC address to IP address. If a BOOTP server is used and the Radio Link Module is reset, the IP address of the Access Point RLM is the same as before the reset.

A Start-up Configuration

A.1 Introduction

Your Radio Link Module comes with installed operating software factory. Together with this software, the RLM has also been loaded with a factory set configuration, that allows for “out-of-the box” operation.

NOTE:

The factory-set configuration should not be confused with a “default” configuration. For example when performing a “Reboot” or “Forced Reload” (described later in this book) the unit will NOT return to the “factory-set” configuration.

To connect to the Radio Link Module, the network parameters of each wireless station should be configured to match the values as identified for the RLM unit.

- When powering up the Radio Link Module for the very first time, these values should match the values listed in Table 9 Start-up Configuration - RLM.
- For normal operation these values should match the ones you identified when configuring the RLM unit. You are advised to record this information on the “Access Point Configuration Record” in this appendix.

A.2 Factory-set Configuration

Table 9 Start-up Configuration - RLM

RLM Parameters		
Access Point IP tab	Obtain an IP address from DHCP server	Enabled
	Default TTL	64
SNMP tab	Read Password	public
	Read/Write Password	public
	System Name	xx-xx-xx-xx-xx-xx [1]
	Trap Host IP address	0.0.0.0 [2]
	Trap Host Password	public
	SNMP IP Access List	<All will be permitted>
Bridge tab	Protocols to Filter	<none>
	Static MAC address Filter	<none>
	Spanning Tree	disabled
	Storm Thresholds	disabled
Access Control tab	(Static) Access Control	<All will be permitted>
	RADIUS Server Access Control	Disabled
Link Integrity tab	Link Integrity	Disabled

1. Ethernet MAC address of the device (printed on a small label on the processor module).

2. No SNMP traps are sent with this IP address.

Table 10 Start-up Configuration - Interface

Wireless Interface		
	Network Name	WaveLAN Network
	RF-Channel	2.462 MHz
	Closed wireless system	Disabled
	Encryption	Disabled
	Medium reservation	Disabled
	Microwave oven robustness support	Disabled
	DTIM period	1
	Distance between APs	Large
	Multicast rate	2 Mbit/s

Table 11 Access Point Configuration Record

Access Point Configuration Record

Common Parameters

Wireless Network

Network Name: _____

Access Control

Access Control ❑ Enabled

Table File Name: _____

RADIUS server ❑ Enabled

SNMP

System Location: _____

IP Subnet Mask: _____

Read Password: _____

Read/Write Password: _____

Access Point Unique Identifiers

Serial Number	MAC Address	IP Address	IF	Frequency	Device Location	Date Installed	Configuration File
			❑E ❑A ❑B				
			❑E ❑A ❑B				
			❑E ❑A ❑B				
			❑E ❑A ❑B				
			❑E ❑A ❑B				
			❑E ❑A ❑B				
			❑E ❑A ❑B				
			❑E ❑A ❑B				
			❑E ❑A ❑B				

Confidential Information
Keep this record in a safe place!

B Troubleshooting

B.1 Introduction

Problems experienced in wireless LAN operation can be related to:

- Configuration mismatch
- Component failure
- Wired or wireless network problems.

B.1.1 Problem-solving Approach

To resolve a configuration mismatch you will need to compare the configuration parameter settings of both RLMs and all stations involved.

To determine a component failure, check the LED activity of the Radio Link Module. You can use the LED Error Table to determine if a problem has a hardware-related cause (component failure). This table may also provide help in diagnosing and solving operational problems that might have other possible causes.

When your RLM appears to have stopped responding to normal bridging requests, you may try to reboot the device as described under Rebooting RLMs. In exceptional cases you may consider to do a forced reload procedure as described in Forced Reload Procedure.

Table 12 LED Error Table

Power	Ethernet	Wireless interface A	Wireless interface B	Description/Action:
⏻	⟷	A	B	
Contin. Green	Flicker Green	Flicker Green	Flicker Green	Normal operation where flickering indicates interface activity. No action required.
	Off	Off	Off	Normal operation that indicates there is no LAN activity • No action required • (Optional) Check if all Ethernet connections are properly installed
Off	Off	Off	Off	No power. • Check the power cord, • Check the power supply

<table>
<tr><td rowspan="3">Contin. Green</td><td rowspan="2">Flicker Green</td><td>Amber</td><td>-</td><td rowspan="3">Network overload.
The Ethernet connection sends more traffic to wireless stations than the RLM Bridge can forward to the interface[1].
Run the RLM Manager Remote Statistics to investigate network performance.
If possible try to eliminate redundant traffic by:
• Filtering protocols
• Setting storm threshold, or
• Shut down Ethernet stations that transmit excessive data</td></tr>
<tr><td>-</td><td>Amber</td></tr>
<tr><td>Green</td><td>Amber</td><td>Amber</td></tr>
<tr><td rowspan="3">Contin. Green</td><td>Flash Red</td><td>-</td><td>-</td><td rowspan="3">Frames are rejected because of an unknown cause.
• Run the RLM Manager Remote Statistics to investigate the number of packets in error.
• If this number is relatively high, run a remote link test to determine which station is causing the packet loss.</td></tr>
<tr><td rowspan="2">-</td><td>Flash Red</td><td>-</td></tr>
<tr><td>-</td><td>Flash Red</td></tr>
</table>

1. When traffic load exceeds the wireless throughput capacity (>11MB/s), the RLM will buffer such requests. In this situation however the buffer is full, and packets are ignored.

Power	Ethernet	Wireless interface A	Wireless interface B	Description/Action:
Amber	Off	Off	Off	Forced reload state. • Proceed with the forced reload procedure as described in C “Forced Reload Procedure” of this Manual.
	Amber	Amber	Amber	
Amber	Flicker Green	Off	Off	Forced reload state. The flickering LED indicate LAN activity on the specific LAN interface. This activity is typically caused by the LAN administrator station that is performing the forced reload. • Proceed with the forced reload procedure as described in C “Forced Reload Procedure” of this Manual.
	Off	Flicker Green	Off	
		Off	Flicker Green	

<table>
<tr><td>Red</td><td>-</td><td>-</td><td>-</td><td>General hardware failure
• Reboot the RLM as described in this Appendix.
• If the problem persists, contact Siemens technical support.</td></tr>
<tr><td rowspan="3">-</td><td>Amber</td><td>-</td><td>-</td><td>Ethernet hardware failure
• Reboot the RLM as described in this Appendix.
• If the problem persists, contact Siemens technical support.</td></tr>
<tr><td rowspan="2">-</td><td>Amber</td><td>-</td><td rowspan="2">SIMATIC NET IWL hardware failure
• Reboot the RLM as described in this Appendix.
• If the problem persists, contact Siemens technical support.</td></tr>
<tr><td>-</td><td>Amber</td></tr>
<tr><td rowspan="2"></td><td rowspan="2"></td><td></td><td>Off</td><td rowspan="2">If the CP 1515 is broken, which can be tested by inserting the card into the SIMATIC NET IWL computer, return the card to your authorized reseller.</td></tr>
<tr><td></td><td>Amber</td></tr>
</table>

B.2 Rebooting RLMs

If a particular Radio Link Module has stopped responding to normal bridging requests, you can reboot (reset) the Access Point RLM. You can reboot RLMs either manually on-the-spot or remotely.

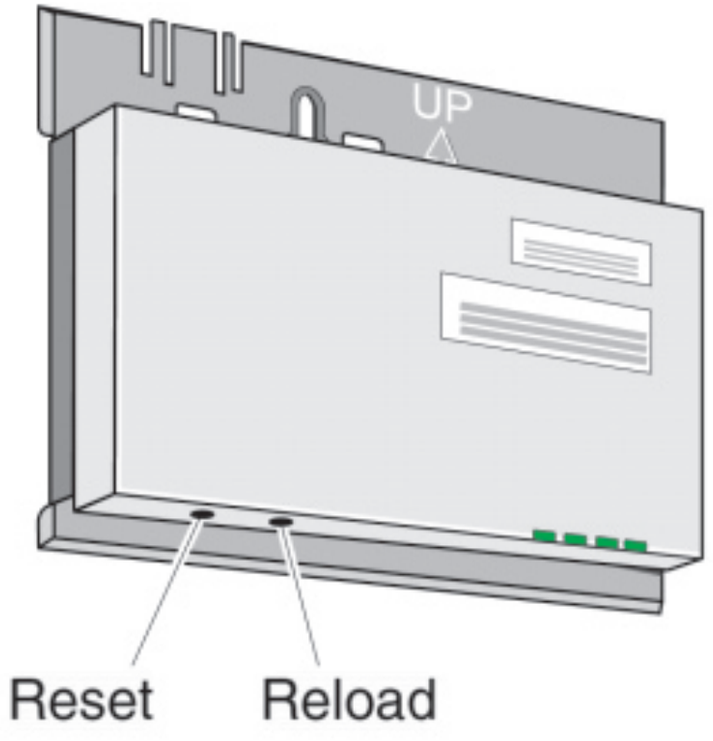
Upon reboot, the Radio Link Module will run the start-up diagnostics and start bridging operation using the configuration parameters as they were stored in the RLM prior to the reboot. For “out-of-the-box” RLMs, these parameters will be as identified in Table 9 Start-up Configuration - RLM.

B.2.1 Manual Reboot

To reboot the RLM manually on-the-spot proceed as follows:

1. Remove the cover of the Radio Link Module (see the Manual “Industrial Ethernet Wireless LAN, Radio Link Module RLM” on IWL-CD that came with your RLM, for assistance if needed).
2. Locate the two small holes on the bottom of the processor module, marked “Reset” and “Reload” as pictured in Figure 43 Reset Button.

Figure 43 Reset Button



3. Use a small pointed object, such as the tip of a ball-point, to press the **Reset** button.

   The RLM will restart and run the start-up diagnostics, characterized by a LED sequence where the LEDs change color in the range Red, Amber, Green.

4. When the Power LED is green, and other LEDs are off or flickering (indicating LAN activity), you can mount the cover of the RLM.

After approximately 15 seconds, the unit will start bridging operation using the configuration parameters as they were stored in the Radio Link Module prior to the reboot.

B.2.2 Remote Reboot

To reboot the Radio Link Module from a remote location:

1. Start the RLM Manager program.
2. Select the target Access Point RLM from the list or enter the IP address for a specific RLM.
3. Open the RLM menu.
4. Select **Reboot** RLM.

   The RLM Manager program will now prompt you to enter the password required to reboot the device.
5. Enter the Read/Write password and click **OK**.
6. The Radio Link Module will restart and run the start-up diagnostics.

After approximately 15 seconds, the RLM will start bridging operation using the configuration parameters as they were stored in the RLM prior to the reboot.

If you would like to display the configuration file or monitor the Radio Link Module's performance after a reboot, you may have to wait until the unit completes the start-up diagnostics before you can access the Access Point RLM again.

C Forced Reload Procedure

C.1 Introduction

A forced reload allows you to recover from a situation where:

- The Radio Link Module has stopped responding to the system
- You have mislaid the unique identifiers such as IP address, SNMP read/ write password, or other parameters that prevent communication with the RLM.
- The Access Point RLM has been configured with incorrect network parameters, preventing you to access the RLM via the network interface.

CAUTION:

When you need to do a forced reload, please keep in mind the following:

a. The RLMs equipped with network interfaces that are set to Forced Reload" mode can not be accessed via the SIMATIC NET IWL network interface.

b. Do not do a "Forced Reload" procedure for more than one Radio Link Module simultaneously.

You might risk unexpected administrative problems due to configuring multiple units with an identical configuration image and IP address.

When in"Forced Reload Mode" the RLM will stop bridging operation. The Access Point RLM is only capable of accepting a new software image to be programmed into the FlashROM.

To access the Radio Link Module in forced reload mode you may need to reconfigure your LAN administrator station.

If your RLM is equipped withCP 1515 cards, you may wish to do the forced reload using a configuration scenario as described in Setting Up your LAN Administrator Station (see either Figure 6 Wired Access via a Network Connection or Figure 8 Wireless Access via an Indirect Connection).

C.2 Doing a Forced Reload

A forced reload procedure consists of three steps:

1. Step 1 - Preparations.
2. Step 2 - Set to “Forced Reload” Mode.
3. Step 3 - Configuring and Uploading Files.

One additional step is optional, but recommended:

4. Creating a Back-up File

C.2.1 Step 1 - Preparations

A forced reload procedure can only be done when you have physical access to the RLM.

- Familiarize yourself with the location of the RLM:
  Do you need special equipment to access the Access Point RLM, such as a ladder or keys to get into the room where the Radio Link Module is located?
- Do you have a back-up copy of the RLMs current configuration file (*.cnf)?
  - If **Yes**, you can use the back-up copy to restore the original configuration.
  - If **No**, you will need to set all the user-defined parameters for the RLM that apply in your network again.

  Back-up copies may have been created upon initial installation using the **Download Config File** option of the RLM Manager program.

- If you have access to the Siemens **http://www.siemens.com/mobic** web site, you can download the latest software (*.bin) available for your Radio Link Module.
- It is advised to specify a temporary IP address for the Access Point RLM. To enter this temporary IP address:
  - — Open the RLM Manager program.
  - — Select from the **Tools** menu the option **Options**.
  - — Enter the temporary IP address in the **Local IP address** field.

  The temporary IP address is assigned to the Radio Link Module in forced reload mode. This is done to enable configuring and uploading the software file, before the Radio Link Module has its definite IP address.

Two configurations of your LAN administrator station are possible to enable you to logically access the RLM:

- Your LAN administrator station is the SIMATIC NET IWL station.
- Your LAN administrator station is a wired (Ethernet) station.

C.2.1.1 Your LAN administrator station is a Wired Station

Your LAN administrator station is connected to the RLM via the Ethernet interface of the RLM.

- Make sure the LAN administrator station and the RLM are connected to the same LAN segment (subnet).

  To communicate with the RLM in “Forced Reload” state, no routers are allowed between the target RLM and the LAN administrator station.
- When using IP addressing, write down the IP address that the Radio Link Module should use.

C.2.1.2 Your LAN administrator station is a Wireless Station

You can use a wireless LAN administrator station to access the Radio Link Module in force reload mode **ONLY IF** the station has indirect access to the RLM, as described on Wireless Access via an Indirect Connection (page 52).

Make sure that your LAN administrator station matches the settings of the RLM that you will use to establish the connection to in forced reload mode.

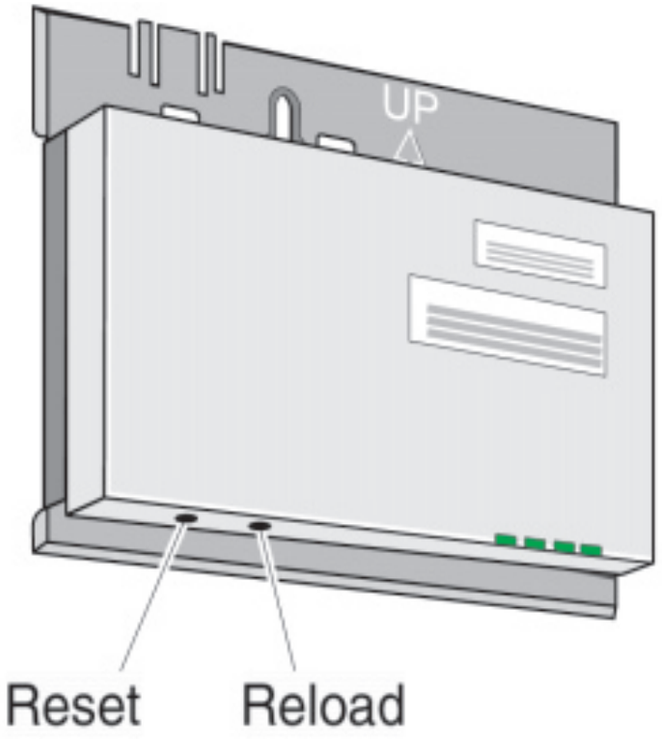
- Make sure the LAN administrator station is within range of the RLM.

When using IP addressing, write down the (new) IP address that you would like to assign to the RLM in forced reload mode.

C.2.2 Step 2 - Set to “Forced Reload” Mode

1. Remove the cover of the RLM.
2. Locate the two small holes on the long-edge side of the processor module, marked “Reset” and “Reload” (see Figure 44).

Figure 44 Reset and Reload Buttons



3. Use a small pointed object, such as the tip of a ball-point, to press the **Reset** button.
4. Release the **Reset** button and wait 5 seconds.

   The Radio Link Module will do start-up diagnostics, characterized by LED activity, where the LEDs will change color in the range Amber, Red and Green.

5. After approximately 5 seconds, use the small pointed object again to press the **Reload** button for approximately 30 seconds.

   You will see the LEDs changing color in the range Amber, Red and Green again.

6. When all LEDs turn Amber, release the **Reload** button.

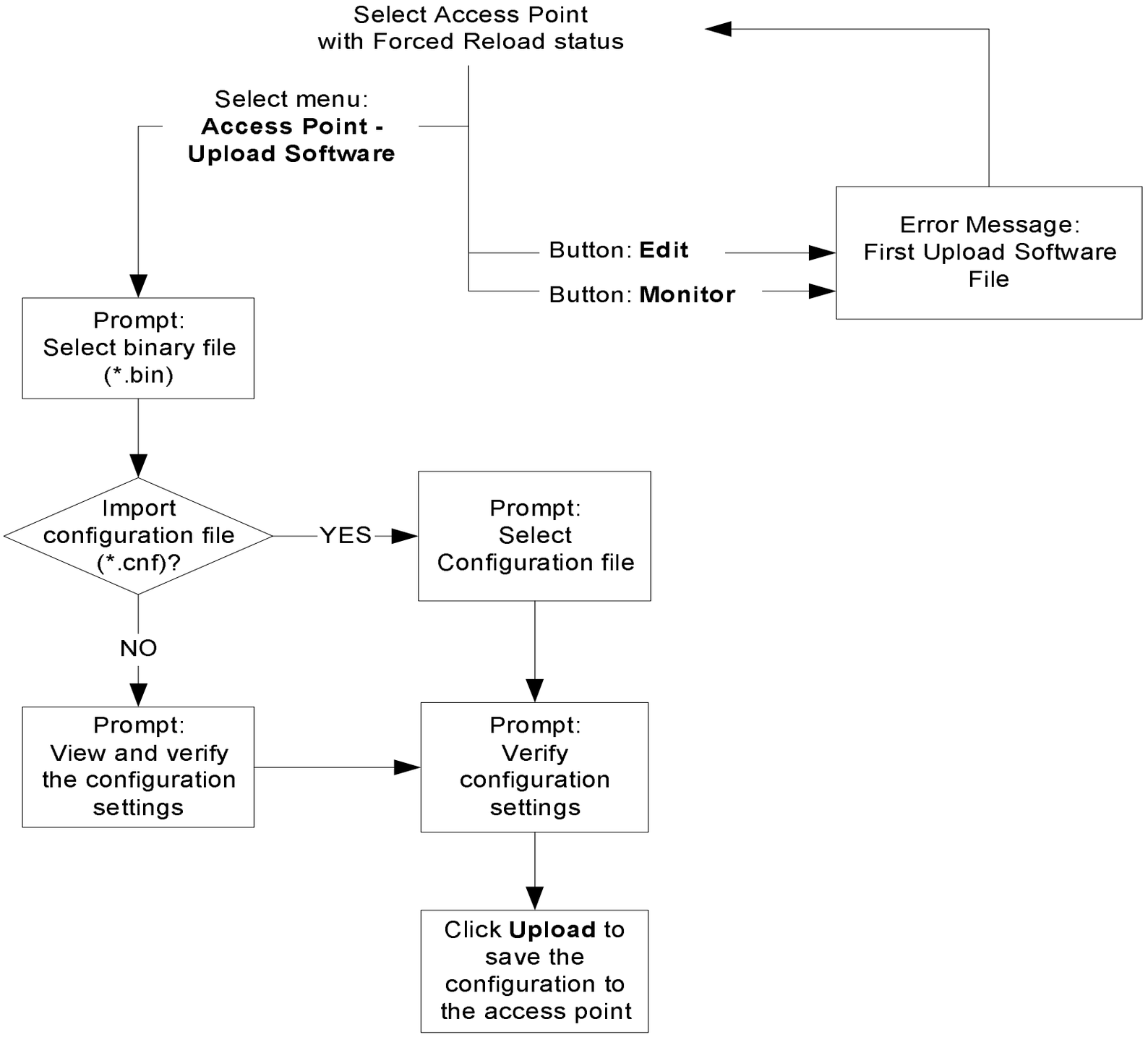
   The Power LED turns to Amber. Other LEDs will be off, or may flicker Green to indicate LAN activity on the associated interface.

7. Start the RLM Manager program and proceed with "Step 3 - Configuring and Uploading Files"

C.2.3 Step 3 - Configuring and Uploading Files

The complete configuration and upload procedure of the forced reload procedure is pictured in Figure 45.

Figure 45 Configuration an upload in forced reload mode


Select Access Point with Forced Reload status
Select menu: **Access Point - Upload Software**
Button: **Edit**
Button: **Monitor**
Error Message: First Upload Software File
Prompt: Select binary file (*.bin)
Import configuration file (*.cnf)?
YES
Prompt: Select Configuration file
NO
Prompt: View and verify the configuration settings
Prompt: Verify configuration settings
Click **Upload** to save the configuration to the access point

Doing a Forced Reload

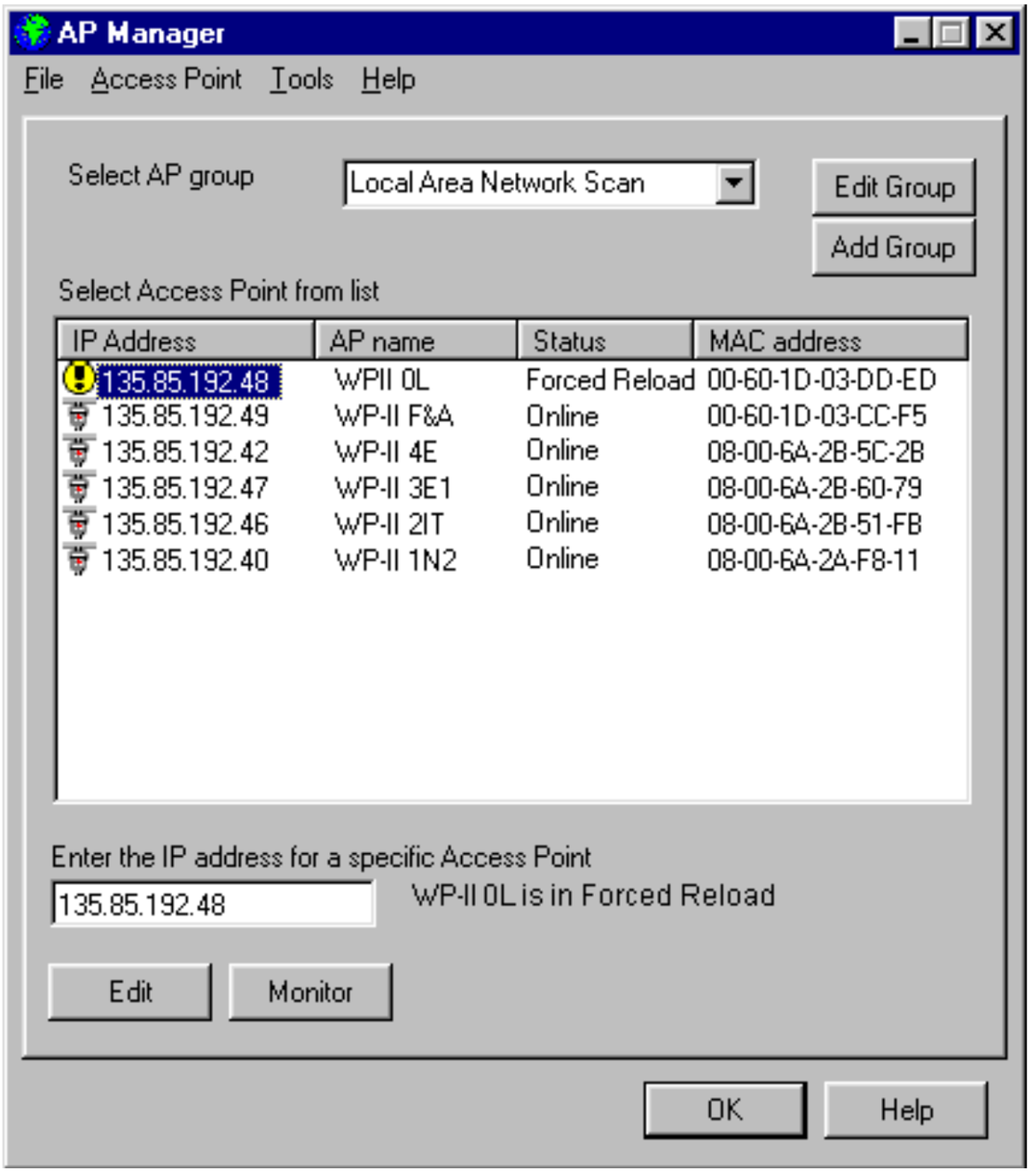
To configure the Radio Link Module in forced reload status and to upload the configuration do the following steps:

1. Select the RLM which is in Forced Reload.

   The Radio Link Module in Forced Reload status is displayed in the main RLM Manager at the top of the list and can be recognized window as follows (see Figure 46):

   - the RLM is marked with the Forced Reload icon,
   - the RLM is marked with the status "Forced Reload", and
   - the RLM has the IP address 153.69.254.254.

Figure 46 The RLM in Forced Reload



2. Select **Upload Software** from the Access Point RLM menu to start the configuration and upload procedure.

- If you click the **Edit** or **Monitor** button before uploading the software, you will be prompted to upload the software first.

3. In the Open window, move to the directory where you have installed the RLM Manager program. If you downloaded the latest RLM software from the Siemens SIMATIC NET IWL web site, select the directory where you saved the downloaded file.
4. From the list of displayed files, select the file "wpnt*xxx*.bin", (where "*xxx*" identifies the version of the RLM software).
5. Click the **Open** button to open the software file.
6. You now have the possibility to upload a back-up configuration file to the Radio Link Module.

NOTE:

When importing a configuration file, make sure you import the correct back-up file. Configuring the Radio Link Module with a configuration file that is identical to the configuration of another Radio Link Module may lead to unpredictable behavior of your network.

- If you **do** have a back-up configuration file and if you **do** wish to use this file to configure the Radio Link Module, click **Yes**.

  Select the back-up configuration file (*.cnf) and click **Open** to open the back-up configuration settings.

  You are advised to check the configuration settings. Click **Ok** to continue.
- If you **do not** have a back-up configuration file, or if you do have a file but **do not** want to use this file to configure the RLM click **No**.

You are now advised to manually modify/verify the configuration settings of the Access Point RLM (i.e. assign a unique IP address, setup the parameters and, (if applicable) the other Access Point RLM identifiers such as the IP Address and SNMP passwords).

7. The Edit Configuration window is displayed. Note that the Edit Configuration window does not contain an **OK** button but an **Upload** button to upload the configuration settings to the RLM.This means that you are editing a local configuration file and that you are not yet connected to the RLM.
8. View (and modify) the configuration settings in all tabs.

   Refer to Basic Network Configuration (page 55) for changing the configuration settings.
9. Click the **Upload** button to upload the new configuration settings to the Access Point RLM in force reload mode.

   The message "Please wait while trying to connect to the RLM" appears. While trying to connect to the Radio Link Module, the IP address in the configuration settings is pinged.
   - Only if the IP address specified in the configuration already exists, you are prompted to enter a new IP address. If the IP address does not yet exists the uploading continues.
   - Because the password of the RLM in forced reload mode is always "public," you do not have to enter this password before uploading information to the Access Point RLM.
10. When prompted to confirm the "Reload of the Remote System," click **Yes** to continue.

The local software file ("wpntxxx.bin") will now import the configuration settings and save these to the software (binary) file. The software file will now be overwritten by the new software file. This does not influence the functionality of the software file. For more information see Upload Software, a Look under the Hood (page 261).

When you want to preserve the original software file, make a back-up copy of this file.

11. You are again prompted to confirm the "Reload of the Remote System." Check the list of parameters displayed thoroughly to make sure all settings are right.
    - If the pop-up window does not display the correct IP address and/or SNMP passwords, click **No** to cancel.
    - If the IP address and/or SNMP passwords are correct, click **Yes** to proceed.
12. The RLM Manager program will upload the new (restored) configuration to your RLM and load it into the FlashROM.

WARNING:
The RLM will reboot and start bridging operation in approximately 60 seconds.

C.2.4 Creating a Back-up File

You are advised to save the configuration parameters of the Radio Link Module to a back-up file (*.cnf). To create a back-up file, use the **Download Config File** option from the Radio Link Module menu.

You are advised to create a back-up file, to anticipate future network errors that might force you to do a forced reload in the future.

Save the back-up file under a name that allows for easy identification in the future.

C.2.4.1 Start-up Diagnostics

On reboot, the RLM will do start-up diagnostics characterized by a LED sequence, where the LEDs will change color in the range Amber, Red and Green.

The start-up diagnostics take approximately 15 seconds. When finished the RLM will start bridge operation characterized by the LED activity. See Troubleshooting (page 236) for more information.

D Upgrading the RLM Software

D.1 About the RLM Software

The Access Point RLM runs on embedded software, that is also referred to as "firmware" or "Bridge Kernel." This software is already factory installed, so in normal situations, you do not need to worry about the software of the RLM.

In exceptional cases however, you may choose to load new RLM software into the FlashROM of your RLMs, for example in situations where:

- You wish to upgrade your RLM to support new functionalities.
- You were advised to do so by Siemens support
- You need to do a forced reload procedure.

The RLM software is a binary file of the format "wpntxxx.bin," where *xxx* identifies the version of the RLM software.

You can find a copy of this file in the program directory where you installed the RLM Manager program. For the latest version of the Radio Link Module software versions you are advised to consult the Siemens **http://www.siemens.com/mobic** web site.

D.2 Upload Software

When uploading RLM software (or firmware) no changes are made to the configuration of the RLM. However, it is recommended to create a back-up file using the **Download Config File** from the RLM menu in case no backup-file exist of the current configuration setting.

1. Select the target Radio Link Module from the list or enter an IP address for a specific Radio Link Module.
2. From the Radio Link Module menu, select **Upload Software**.
   The RLM Manager program will prompt you to open an Access Point RLM software file (*.bin).
3. Move to the directory where you have installed the RLM Manager program file, or the directory where you saved the Access Point RLM software file you downloaded from the Siemens SIMATIC NET IWL web site.
4. From the list of displayed files, select the file "wpntxxx.bin," where "xxx" identifies the version of the Access Point RLM software.
5. Click the **Open** button to open the Radio Link Module software file.
6. Enter the password for the RLM if you are prompted to and click **OK** to continue.
7. When prompted to confirm the RLM software upload, click **Yes**.

WARNING:
The RLM will now reboot and start bridging operation using the parameters as set in the software file.

D.2.1 Confirm Upload RLM Software

When you try to upload the RLM software file (*.bin) to your RLM, a message box will pop-up asking you to confirm:

- The upload to the RLM, and
- Overwriting the RLM software file (*.bin) that you selected for upload to the RLM.

You do not need to be concerned that the RLM software file will be overwritten, as this will affect neither its functionality nor its features.

D.2.1.1 Yes, Upload RLM Software

When you select "Yes, Upload Access Point RLM Software," the RLM Manager program will:

1. First save the Radio Link Module software file back to disk, using the same filename, i.e. the software file you opened will be overwritten.
2. Next use the saved file to upload the target Radio Link Module.

When the RLM software file is saved to disk, the "Configuration Parameter Area" of the software file is updated with the settings that were retrieved from the RLM or imported from the back-up file (*.cnf). The "Software Area" of the RLM software file remains unchanged (for more information, see Upload Software, a Look under the Hood (page 261).

As the "Software Area" remains unchanged, overwriting the software file does not affect the functionality or the features of this software file.

D.2.1.2 No, do not Upload RLM Software

When you select "No, do not Upload RLM Software," the RLM Manager program will abort the upload operation.

If you would still like to upload the RLM software, but hesitate to overwrite the original software file, you are advised to make a back-up copy of the original software file (*.bin) and save it to a separate (floppy) disk drive.

D.2.2 Upload Software, a Look under the Hood

Actually the Radio Link Module software file consists of two information areas that are both stored in the FlashROM of the Radio Link Module Bridge:

1. The actual software program area. The data in this area can not be configured by the end-user.
2. The Configuration Parameters area that contains user-defined settings of the Radio Link Module. The data in this area can be modified at any moment when you use the RLM Manager program to open and save a remote config file.

What actually happens in the procedure to upload Radio Link Module software, is that the RLM Manager program will merge the configuration parameters retrieved from the RLM with the software information from the RLM software file (*.bin). These will be saved to disk first, prior to uploading the information into the RLM.

E Further Support

E.1 Who to contact

If you have technical questions about using the described product and your problem is not dealt with in the documentation or in the integrated help system, please contact your Siemens representative or dealer.

You will find the addresses:

- in our catalog IK PI or CA01
- on the Web (http://www.siemens.com/simatic-net)

E.2 Automation and Drives, Service & Support

Service & Support from A&D is available round the clock worldwide.

The languages spoken are German and English.
French, Italian, and Spanish are also spoken on the authorization hotline.

Figure 47 Service and Support

Technical Support	**Authorization Hotline**
Europe and Africa (Nuremberg) Mo. to Fr. 7:00 to 17:00 (local time, GMT +1) Phone:+49 - (0) 180 - 5050 - 222 Fax:+49 - (0) 180 - 5050 - 223 E-mail:techsupport@ad.siemens.de	**Europe and Africa** (Nuremberg) Mo. to Fr. 7:00 to 17:00 (local time, GMT +1) Phone:+49 - (0) 911 - 895 - 7200 Fax:+49 - (0) 911 - 895 - 7201 E-mail:authorization@nbgm.siemens.de
America (Johnson City) Mo. to Fr. 8:00 to 19:00 (local time, GMT -5) Phone:+1 - (0) 423 - 262 - 2522 Fax:+1 - (0) 423 - 262 - 2231 E-mail:simatic.hotline@sea.siemens.com	
Asia and Australia (Singapore) Mo. to Fr. 8:30 to 17:30 (local time, GMT +8) Phone:+65 - (0) 740 - 7000 Fax:+65 - (0) 740 - 7001 E-mail:simatic.hotline@sae.siemens.com.sg	

SIMATIC Premium Hotline	
Worldwide (Nuremberg) Workdays 0:00 to 24:00 (local time, GMT +1) Phone:+49 - (0) 911 - 895 - 7777 Fax:+49 - (0) 911 - 895 - 7001 E-mail:techsupport@ad.siemens.de	Fast callback guaranteed within a maximum of two hours (charged, only with the SIMATIC Card)

E.3 Service & Support on the Internet

On the World Wide Web, you will find the very latest information on the entire SIMATIC product range, for example, answers to frequently asked questions (FAQs), Tips and Tricks, software updates, and user information.

In addition to this free information, you can also order the following, for which a charge is made:

- Software products
- Sample application programs

These are charged to the SIMATIC CARD.

Internet address:

http://www.siemens.de/automation/service&support

You can also formulate a question for the SIMATIC Knowledge Manager that will find the solution in the knowledge database.

If you are working in an area without an online connection, part of the free information area is available on the "SIMATIC Customer Support Knowledge Base" CD.

E.4 Training for SIMANTIC NET

Who to Contact about Training Courses:

Siemens AG
Trainings-Center für Automatisierungs- und Antriebstechnik
A&D PT 49 Kursbüro

Östliche Rheinbrückenstraße 50
76181 Karlsruhe
Germany

Phone: +49 - (0) 721 - 595 - 2917

Fax: +49 - (0) 721 - 595 - 6087

Internet: http://www.sitrain.com

E.5 Certification

The products of SIMATIC NET are manufactured and marketed using a quality management system complying with DIN ISO 9001 and certified by DQS (certificate registration no. 2613). The DQS certificate is recognized in all IQNet countries (Reg. No. 2613).

Glossary

A

Access Control

A security feature for RLM that enables you to restrict wireless access to a access point to authorized stations only.

Authorized stations are identified by the MAC address of their SIMATIC NET IWL PC Card in a so-called 'Access Control Table' file that is loaded into the SIMATIC NET IWL access points as part of the configuration

When Access Control is enabled, the Radio Link Module will ignore all requests to forward data to/from SIMATIC NET IWL devices that are not identified in the Access Control Table. You can create or edit Access Control Table files using either the RLM Manager or the CP 1515 program.

Access Control Table

ASCII table that contains all the MAC Addresses of stations authorized to send/receive data via the Radio Link Module. To build an Access Control Table you can use the RLM Manager program.

The Access Control Table is loaded into the Radio Link Module as part of an configuration upload.

Analysis Polling interval

A parameter that enables you to control the responsiveness of the SIMATIC NET IWL RLM Manager Remote Link Test. The Analysis Polling Interval determines how often RLM Manager will read the diagnostic tallies of the bridge unit. Valid values: 1-15 seconds.

See also: Monitoring your SIMATIC NET IWL Network (page 67)

B

Basic Access Network

A basic access network consists of a small sized wireless LAN, with no connections via gateways or routers. The number of RLM in this network typically varies between 1 and 5. The administrator stations need to have the TCP/IP protocol stack loaded and use IP addressing to configure and monitor the RLMs. IP addressing and the TCP/IP protocol are not strictly necessary for client stations.

Beacon

A message that is transmitted at regular intervals by the RLM to all wireless stations in the domain. Beacon messages are used to maintain and optimize communications by helping mobile SIMATIC

NET IWL stations to automatically connect to the access point that provides the best communications quality.

BOOTP (Bootstrap Protocol)

The standard protocol that is used to configure systems across internetworks.

BootROM

Memory chip in your Access Point RLM that contains the start-up configuration of the access point. When you change the configuration of a RLM unit, the values of the configuration parameters will be stored in the BootROM.

Bridge in

The total number of data packets arriving at the RLM from the LAN segment served by the selected wireless network interface.

This number reflects the sum of Unicast and Non-Unicast packets.

See also: RLM Manager, Monitoring, Remote Statistics

Bridge in discards

The number of data packets not accepted by the RLM.

See also: RLM Manager, Monitoring, Remote Statistics

Bridge out

The number of data packets that have been forwarded by the RLM to the LAN segment served by the selected interface.

See also: RLM Manager, Monitoring, Remote Statistics

Bridge Priority

A Bridge setup parameter that enables you to influence the choice of the 'Root Bridge' and the 'Designated Bridge' as calculated by the Spanning Tree Algorithm. A low numerical value of the Bridge Priority Parameter makes the bridge more likely to become the designated bridge or Root Bridge (typically '0'). The recommended value is '32768'. Valid values: 0-65000, Initial value: '32768'.

See also: RLM Manager, Setup Bridge Parameters

Broadcast

Messages transmitted by a single station (typically a server) to all stations on the network. This type of traffic is also referred to as Non-Unicast messages.

Bytes in

The number of bytes (octets) received at the RLM from the LAN segment served by the selected wireless network interface, including framing characters.

See also: RLM Manager, Monitoring, Remote Statistics

Bytes out

The number of frames requested by higher level protocols that are to be transmitted to a Non-Unicast address (i.e. a subnetwork broadcast or subnetwork Multicast address). This number includes the frames that were discarded or not sent.

See also: RLM Manager, Monitoring, Remote Statistics

C

Collisions

The number of packets that were not received properly as a result of a collision, due to multiple stations trying to send packets over the medium simultaneously.

See also: RLM Manager, Monitoring, Remote Statistics

D

DHCP (Dynamic Host Configuration Protocol)

DHCP is a Microsoft proprietary extension to the existing bootstrap protocol (BOOTP). DHCP enables a LAN administrator to have a network server configure workstations with an IP address dynamically without further intervention.

A dynamically assigned IP address is referred to as an 'Active Lease'. The Active Lease usually has an expiry date, which allows re-allocation of IP addresses that are no longer used.

For Radio Link Modules you are advised to use a specific IP address for which there is no expiry date. To do so, you can use your DHCP management program to reserve the IP address or a range of IP addresses.

For network devices that require a specific IP address, or for which you do not want the 'IP address lease' to expire, you can use a DHCP Management program to reserve their IP addresses. This is the case with your Radio Link Modules.

Once a range of IP addresses has been reserved, you can use the values in this range to assign to your SIMATIC NET IWL system.

The Unique Identifier is the Media Access Control (MAC) address for the DHCP Client. The Client Name should be the computer name for the DHCP Client. However, this name is used for identification purposes in the DHCP Manager interface and, therefore, does not have to be and will not affect the actual computer name.

To see which IP addresses are still available, your DHCP Management program will usually include a 'Scope Active Leases' option. This option allows you to see which DHCP Clients have leased an IP address from the DHCP Server.

E

Encryption

A security feature for Access Point RLM and SIMATIC NET IWL stations that enables you to encrypt data that is transmitted via the wireless medium.

SIMATIC NET IWL products are optionally available with a factory-installed encryption chip that is based the WEP encryption algorithm.

To use encryption in your wireless network, all SIMATIC NET IWL stations and access points must have the encryption feature installed and set to 'Enable'. All Radio Link Modules and SIMATIC NET IWL devices in the network environment must use the same encryption key.

The encryption key consists of 16 hexadecimal numbers in the range 0-9, A-F. The second digit of each pair must be even (0,2,4,6,8,A,C,E).

Enterprise-wide Network

A network configuration that has the scale of a corporate LAN. This type of network may include network segments in different departments, interconnected by means of bridges and routers. When the network comprises gateways, routers or bridges, each network device must be identified by a unique IP address. The network may extend to wireless networking in different buildings, where the buildings are connected by a wired link, e.g. a leased line.

F

Filter Aging Time

Radio Link Modules maintain dynamic lists to identify the interface where they last spotted a SIMATIC NET IWL station (either the Ethernet interface, or SIMATIC NET IWL interface A or B).

When the RLM receives a packet addressed to a specific station, this list will help to determine to which interface the packet should be bridged.

When mobile stations roam between multiple cells this table will be updated automatically.

When there is no traffic from or to a specific station for a longer period of time (for example when a station was shut down), the Filter Aging Time determines how long the access point will ‘remember’ the location of this SIMATIC NET IWL device.

Firmware

Basic operating software for SIMATIC NET IWL PC Card and Radio Link Module that is factory-installed.

Occasionally firmware upgrades may become available when new functions or features are developed for your SIMATIC NET IWL product.

Firmware Upgrade

Upgrade for the embedded software on the hardware of your SIMATIC NET IWL product.

- For SIMATIC NET IWL PC Card, firmware upgrades are distributed as an executable file of the format "wsuVVxxx.exe," where "xxx" identifies the version of the upgrade. This executable file is run once on the computer containing the PC Card.
- For Access Point RLM, firmware upgrades are distributed as a binary file of the format "wpntxxx.bin," (where "xxx" identifies the version of the firmware. To upgrade the firmware of the Radio Link Module, use the **Upload Software** option of the acess point menu of your RLM Manager program.

Forward Delay

A timer for the 'Spanning Tree Algorithm' that prevents a bridge to forward data packets when:

- The bridge receives information that the active Spanning Tree topology must be updated (for example when a bridge breaks down or when somebody modified the 'Bridge Priority' or 'Path Cost' value of a particular bridge);
- the bridge registers that the protocol information exceeds the specified 'Max. Age' value.

Changes in the Spanning Tree topology must be communicated to all bridges in the bridged network. The Forward Delay timer will

compensate for the propagation delays that occur in passing the protocol information, allowing all bridges to close the old data paths, before the new data paths are activated.

Recommended value: 15 seconds

H

Hello Time

A Spanning Tree parameter that identifies the time interval between Configuration BPDU messages as transmitted by a root bridge or a bridge that is attempting to become the root bridge.

Recommended value: 2 seconds.

I

Initiator Station

The (remote) Access Point RLM device that you selected to initiate a Remote Link Test with a wireless station connected to the selected Radio Link Module.

The Remote Link Test Partner can either be a wireless station, or another RLM unit.

IP Address

The Internet Protocol (IP) address is a unique addressing code for computing devices. When your network already uses IP addressing, you must change the factory-set IP address to a value selected from the range of IP addresses assigned to your organization.

K

Kernel

See 'Firmware'

L

LAN Segment

A logical area within a network that is connected with other areas via a bridge.

For Radio Link Modules, these areas can either be an Ethernet or a SIMATIC NET IWL segment. For Access Point RLMs there could even be two SIMATIC NET IWL segments (A and B). Each SIMATIC NET IWL segment is identified by a unique NWID.

Link Test

An SIMATIC NET IWL diagnostics option that enables you to investigate a specific link between two wireless stations.

You can use the Link Test to analyze the quality of the wireless communication, and to determine or optimize the placement of stations and antennas.

M

MAC Address

16-digit hexadecimal number that identifies a networking product on the network.

MAC Address Filter

An advanced Bridge setup parameter for Radio Link Modules that enables you to deny data traffic between two specific devices via the wireless interface(s) of the access point bridge.

You can use the Static MAC Address filter to optimize the performance of a wireless (and wired) network.

For example, to prevent redundant traffic from being transmitted over the wireless network, you could deny traffic between two particular servers, identified by their MAC Address and their location as perceived by the Access Point RLM (on the 'wired' or wireless' port of the bridge).

In most situations, however, it will be easier to control redundant traffic via other filtering options, such as 'Protocol Filtering.

Max Age

An advanced Bridge setup parameter for Radio Link Module that identifies the maximum age of received Spanning Tree protocol information.

When the bridge receives protocol information that exceeds the Max Age value, the bridge will discard the information and start the Forward Delay timer to allow other bridges to forward updated topology information, e.g. that another bridge has become the Root Bridge.

Recommended value: 20 seconds.

Multicast

Messages transmitted by a single station (typically a server) to multiple stations on the network. This type of traffic is also referred to as Non-Unicast messages.

Multicast Mechanism

In network environments that include several RLMs, the Multicast Mechanism avoids frame collisions when several access points try to access the wireless medium at the same time, for example in case of messages that are transmitted from one station to multiple stations (Multicast) or all stations (Broadcast) on the network.

The default Multicast Mechanism generates a random delay for each wireless interface of a Radio Link Module. The random delay is based

on the last digits of the MAC address of the inserted SIMATIC NET IWL PC Card.

Optionally you can define a 'User-defined' Multicast delay in the range of 1-10.

See also: RLM Manager Edit parameters

N

Noise Level

The Noise level is the level of local background noise as measured at the wireless interface of a Access Point RLM. The Noise level counter reflects only the Noise Level value (in %) of the latest frame that was received on the interface.

See also: CP 1515 Link Test

Non-Unicast packets in

The number of Non-Unicast packets delivered to a higher protocol, typically Multicast or Broadcast messages.

See also: RLM Manager Remote Statistics

Non-Unicast packets out

The number of packets requested by higher level protocols, to be transmitted to a subnetwork-unicast address, typically Multicast or

Broadcast messages. This number includes the frames that were discarded or not sent.

See also: RLM Manager Remote Statistics

O

Out Collisions

The number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one or more collisions plus the number of collisions detected on a particular interface later than 512 bit-times into the transmission of a packet.

See also: RLM Manager Remote Statistics

P

Packets received/lost

The ‘Packets received/lost’ counter displays the percentage of packets received relative to the number of packets expected. The ‘packets received/lost’ counter is only displayed when you select the View Details option.

See also: CP 1515 Link Test

Path cost

An advanced Bridge Setup parameter for Radio Link Module that is used to determine the preferred data paths between bridges throughout the network and the root bridge as calculated by the 'Spanning Tree Algorithm.

The 'Root Bridge' transmits BPDU messages throughout the Local Area Network. When a bridge unit receives a BPDU message at one of its ports, it will add the value in the "Path Cost" field for that port to the value in the 'root path cost field' of the BPDU message prior to forwarding the message again. This will help the other bridges to determine the 'Total Path Cost' to the Root Bridge via this port.

A lower 'Path Cost' value would typically be used for ports to LAN segments closer to the Root Bridge. A higher 'Path Cost' value would typically be used for ports to LAN segments that are 'the leafs' of the Spanning Tree.

For example, when you use the Access Point RLM as an access point for wireless stations to the Ethernet, a high 'Path Cost' for the SIMATIC NET IWL port will minimize unnecessary use of the bandwidth for the wireless medium (recommended value 500).

Peer-to-Peer Workgroup

A stand-alone workgroup of wireless stations which participate in a small (Peer-to-Peer) network. This is typically a SIMATIC NET IWL network configuration without RLMs that could connect the stations into a network infrastructure.

The stations must be configured to operate in Peer-to-Peer mode.

Port Priority

An advanced Bridge Setup parameter for Access Point RLM that enables you to influence which port should be included in the Spanning Tree, when concurrent bridge ports of a single bridge unit are connected in a loop.

A lower value makes a port more likely to become selected in the Spanning Tree than the concurrent one that has a higher numerical value. Valid values: 0-255. Initial value: ‘128’

R

Read Password

A security option that enables you to create a network management level by means of a password.

For example, the ‘Read Password’ in combination with the correct IP address will authorize a local LAN administrator to display only the RLM Manager Monitor function for a specific access point, but not to view or modify the access point configuration.

You can set the ‘Read Password’ using the SNMP tab in the RLM Manager program.

Read/Write Password

A security option that enables you to create a network management level, by means of a password.

For example, the ‘Read/Write’ password in combination with the correct IP address will authorize a Corporate LAN Administrator to display all RLM Manager Monitor functions and to display or edit the Radio Link Module configuration.

You can set the ‘Read/Write’ password using the SNMP tab in the RLM Manager program.

Remote Link Test

A SIMATIC NET IWL diagnostics option of the CP 1515 program. You can use the Remote Link Test to analyze the Link Quality between a remote RLM and a station connected to the selected Radio Link Module unit.

This option is often used to investigate wireless outdoor links, or to analyze the Link Quality of wireless stations in a remote network.

Roaming

Roaming is a function that enables mobile SIMATIC NET IWL devices to migrate between different physical locations within the LAN environment.

To allow roaming each of these locations must be services by a Access Point RLM.

The roaming functionality will monitor the communications quality with the RLMs and, if required, automatically connect to another access point to maintain the network connection.

Roaming is only possible within one domain, i.e., as long as the mobile station is within range of Radio Link Modules that are identified by the same Wireless Network Name.

S

Signal Level

The signal level indicates the strength of the SIMATIC NET IWL signal as received at the wireless network interface.

Site Monitor

A SIMATIC NET IWL diagnostics option of the CP 1515 program that enables you to display the communications quality of multiple Access Point RLM units simultaneously. You can use the Site Monitor to investigate the overall coverage of your SIMATIC NET IWL network, and to perform site verifications.

Site Verification

A procedure to determine or optimize the placement of your Radio Link Module.

See also: Site Monitor.

SNMP (Simple Network Management Protocol)

A standard network protocol that can be used to manage networks locally, or worldwide via the Internet.

SNMP IP Access List

An advanced Security option that enables you to authorize SNMP management to a restricted group of SNMP Management stations.

To authorize a station to access the Radio Link Module configuration or diagnostic information, you will need to add the IP address of that station to the so-called SNMP IP Access List.

When you enable the SNMP IP access option, the RLM will deny all requests to read the configuration data or diagnostic tallies when the IP address of the requesting station is not registered in the SNMP IP access list.

You can use the SNMP IP Access List in combination with other security options such as the ‘Read’ and ‘Read/Write’ passwords.

To create or edit the SNMP IP Access List, use the SNMP tab of the RLM Manager program.

SNMP Polling Interval

A parameter that enables you to control the responsiveness of the RLM Manager Monitor options. Valid values: 1 second - 5 minutes.

SNMP Trap Messages

SNMP trap messages are part of the trap host mechanism which can be used to inform a network administrator when somebody resets a Access Point RLM unit, loads a new configuration into the access point, or performs a forced reload procedure.

The trap host alert message will enable the network administrator to verify whether this was an authorized action or not.

To receive the Trap Alert messages, the management station needs to have a standard Trap Host Agent installed to handle the trap messages.

SNR (Signal to Noise Ratio)

The Signal-to-Noise Ratio (SNR) is the primary diagnostic counter to diagnose wireless performance. The SNR indicates the relative strength of the received Signal Level compared to The Local Noise Level.

Spanning Tree

An advanced Bridge setup option for complex network topologies that enables you to enhance data traffic efficiency and eliminate the possibility of data loops.

With the spanning tree algorithm, all bridges on the LAN exchange special configuration messages that allow them to:

- Elect a single bridge among all bridges in the connected LAN segments to be the root bridge.
- Calculate the distance of the shortest path to the Root Bridge.
- Elect a 'Designated Bridge' in each LAN segment that will forward packets between that LAN segment and the Root Bridge.

Select a 'Root Port' among all ports of the bridge unit.

The spanning tree algorithm enables bridges to calculate a loop-free subset of the LAN topology (a tree) that provides the most efficient level of connectivity between every pair of physically connected Local Area Network segments.

If the 'shortest data path' fails, (for example as a result of a physical breakdown), the Spanning Tree will automatically rebuild the topology within the confines of the available bridged LAN components.

Station address

The station address is a unique identification designator stored in each SIMATIC NET IWL PC Card and Radio Link Module. The addressing system used for station addresses conforms to the universal MAC addressing convention. The station address is a 12 digit, alphanumeric code, arranged as 6 digit pairs of hexadecimal numbers (see also ""MAC Address"")

Station Name

The station name is an optional parameter that may be used to designate wireless devices in the network. The name can help to identify a device in one of the SIMATIC NET IWL diagnostic utilities. A station name can consist of up to 31 alphanumeric characters.

Storm Threshold

An advanced Bridge setup option that you can use to protect the network against data overload by:

- Specifying a maximum number of frames per second as received from a single network device (identified by its MAC address).
- Specifying an absolute maximum number of messages per port.

The 'Storm Threshold' parameters allow you to specify a set of thresholds for each port of the Radio Link Module, identifying separate values for the number of broadcast messages/second and Multicast messages/second.

When the number of frames for a port or identified station exceeds the maximum value per second, the access point will ignore all subsequent messages issued by the particular network device, or ignore all messages of that type.

Subnet

A subnet is a logical sub-division of a Local Area Network that has been divided by means of routers or gateways. A subnet may include multiple LAN segments.

Each subnet is identified by the Subnet Mask.

Note: SIMATIC NET IWL roaming does not work over routers. To allow mobile stations to roam between different wireless cells, all wireless stations and access points must be connected to the same LAN subnet.

T

TTL (Time-To-Live)

An advanced IP Parameter Setup counter that you can you use to maintain network efficiency. The purpose of the Time To Live counter (TTL) is to avoid endless forwarding of message frames with an incorrect address that pollute the network medium.

The TTL defines a maximum number of passes per hop. Each time the frame is forwarded by a router, the TTL counter decreases by one. When the TTL = 0, the frame is rejected.

U

Unicast packets in

The number of subnetwork-frames delivered to a higher protocol. This is ‘true data’ from station to station.

Unicast packets out

The number of bytes (octets) transmitted out to the interface.

This is ‘true data’ from station to station.

Up Time

The amount of time elapsed since the last time the RLM unit was powered up, reset, or uploaded with a new configuration.

W

Windows workgroup

A Windows workgroup can consist of either wireless or wired network connections or a combination of the two. Usually a Windows workgroup consists of members who are related because of a shared function, e.g. members of the same department. For a Windows workgroup it is not relevant where the workgroup participants are located, since the members of a Windows workgroup are identified by their workgroup name only.

Index

A

Access Control
  disable 164
Access Control Table 161
  manual setup 179, 180
Advanced Parameters 191
Analysis Polling Interval 113
Analyzing Link Quality
  see Link Test Results 77

B

Back-Up
  configuration files 246, 257
  create file 224
BOOTP 231
Bridge In Packets 110
Bridge Kernel 258
Bridge Out Packets 110
Bridge Parameters 197

C

Carrier Sense Multiple Access/
  Collision Avoidance 131
Carrier Sense, see CSMA/CA 146
CD-ROM
  files on 23
Client Manager 71
Component Failure 236
Configuration
  back-up 224
  mismatch 236
  upload 224
Configurations
  access point 24
  advanced 24
  multiple channel 29

stand alone wireless LAN 26
Configuring Access Point
scenarios 47
wired station 48, 49
wireless station 50, 52
Configuring access point
wireless station 51
CP 1515 Manager
about 19
Site Monitor 82
CSMA/CA 131, 146
CTS
see Medium Reservation 134

D

Default Router 210
DHCP 45, 231
Distance Between APs 194
Download Config File 66, 228
Dual PC Card Configuration 229

E

Encryption
see Wired Equivalent Privacy 167
Ethernet
configuration scenario 47
connecting to 27
Ethernet Interface
selecting 216

F

Firmware 258
Forced Reload
mode 244, 245
procedure 244, 250
Frequency
channel separation 31

H

Help
on-line 22

I

Icons
used in this document 22
In Errors 110
Initiator Station 104
Interface Parameters 63
Interference Robustness 193
IP Access List, SNMP 215
IP Address
about 229
access point 50, 53
edit 62
MANAGER station 45

K

Kernel 258

L

LAN Administrator Station
see MANAGER Station 32
LED
error table 237
Link Test 74
logging measurement data 92
selecting link test partner 81
test results 77
Logging
automatic 93
manual 93
Logging Measurement Data
stop 95

M

MAC Address
access control 160
access point 49
MANAGER Station
introduction 32
wireless station 39, 50
Manual Data Logging 93
Measurement Data
automatic data logging 93
automatic logging 93
logging 81, 90, 92

logging options 93
manual logging 93
Medium Reservation
CTS 136
RTS 136
threshold 136
Monitoring
CP 1515 Manager 68
introduction 67
methods 71
RLM Manager 98
utilities 67
Multicast Rate 196

N

Network
basic access 58
managing 67
name 63
performance 67
problems 236
Network Name 63
Non-Unicast Packets
see also traffic 117

O

Optimization
redundant traffic 117
Out Collisions 110
Out Errors 110

P

Parameters
advanced 191
changing common 227
network name 63
RTS/CTS medium reservation 131
wireless interfaces 63
Performance 67
Preventing Unauthorized Access 155
Protocol Filtering 200

R

RADIUS Server Access Control 165
Ratio of Errors to Bridge Packets 110
Read Password 177, 233
Read password 177
Read/Write Password 177, 233
Reboot
  manually 241
  remotely 243
Redundant Traffic 117
Refresh Button 105
Remote Link Test 103
Remote Statistics 98
Reset, see Reboot 241
RLM Manager 98
  about 19
Roaming 229
RTS
  see Medium Reservation 134

S

Securing Unauthorized Access 155
Security
  access control 159
  data encryption 167
  read password 177
  SNMP IP access 178
  trap host alerts 180
  WEP Encryption 168
  write password 178
Setup
  bridge parameters 197
SIMATIC NET IWL
  install software 40
Site 81
Site Monitor 81
  logging measurement data 92
  selecting another domain ID 86
SNMP
  default router 210
  IP access list 215
  IP address access list 177
  parameters 211

polling interval 113
read password 213
SNR (Signal to Noise Ratio) 84
Spanning Tree 203
SSID 90, 97
Static MAC Address Filter 202
Storm Threshold 205
Subnet Mask 46, 210
Subnets
about 229
System Interval Parameters 112

T

TCP/IP Protocol Settings 43
Technical Support 262
Time Interval 112, 114
Time To Live 211
Tools
CP 1515 Manager 19
RLM Manager 19
Traffic
payload 117
traffic load 117
Trap Host 210
activate 181
alerts 180
disable 180
IP address 214
mechanism 180
password 180, 215
Trap Messages 210
Troubleshooting
problem-solving approach 236

U

Unicast Packets
see also Traffic 117
Up Time 101
Upgrade
access point software 258
Upload Software 253, 259
about 261
Utilities 67

W

WEP 167
see Wired Equivalent Privacy 167
WEP Encryption 168
Wired Equivalent Privacy 167
Wireless Interface Parameters 63
Wireless Network
setting parameters 63